UNIVERSIDADE TIRADENTES – UNIT
CURSO DE GRADUAÇÃO EM DIREITO
TRABALHO DE CONCLUSÃO DE CURSO – ARTIGO CIENTÍFICO

LEI GERAL DE PROTEÇÃO DE DADOS: OS RISCOS DA NÃO ADEQUAÇÃO E OS PROGRAMAS DE *COMPLIANCE*

Anna Paula Resende Novais Pereira

Orientador: Rafael Soares de Cerqueira

ARACAJU

2020

ANNA PAULA RESENDE NOVAIS PEREIRA

LEI GERAL DE PROTEÇÃO DE DADOS: OS RISCOS DA NÃO ADEQUAÇÃO E OS PROGRAMAS DE *COMPLIANCE*

Trabalho de Conclusão de Curso – Artigo Científico - Apresentado ao Curso de Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do grau de bacharel em Direito.

Aprovado em _____/_____/_____.

Banca Examinadora

Rafael Soares de Cerqueira
Orientador
Universidade Tiradentes

Alex Daniel Barreto Ferreira
Universidade Tiradentes

Valquiria Nathali Cavalcante Falcão
Universidade Tiradentes

LEI GERAL DE PROTEÇÃO DE DADOS: OS RISCOS DA NÃO ADEQUAÇÃO E OS PROGRAMAS DE *COMPLIANCE*

GENERAL DATA PROTECTION LAW: THE RISKS OF NON-ADEQUATION AND COMPLIANCE PROGRAMS

Anna Paula Resende Novais Pereira[1]

RESUMO

A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) no Brasil trouxe grandes mudanças a serem realizadas pelas corporações, principalmente na forma como as empresas armazenam e tratam os dados coletados. Por essa razão, o presente artigo objetiva mostrar os riscos que incorrem as empresas que não se adequam à LGPD, bem como as formas de entrar em conformidade, em especial, através de eficientes programas de *compliance*. Para tanto, fora utilizada uma abordagem qualitativa, com objetivos exploratórios, através de procedimentos de coleta de informações, através, principalmente, de pesquisas bibliográficas e de consulta a legislação. Observou-se, por sua vez, que os riscos da não adequação são potencialmente altos e prejudicam, em demasia, as empresas, fazendo-se necessária a adaptação das corporações à legislação vigente por meio de programas como o *compliance*, que garante a observância da lei e melhora a gestão dos riscos da atividade exercida pela empresa.

Palavras-chave: LGPD. Não Adequação. *Compliance*.

ABSTRACT

The implementation of the General Data Protection Law (GDPL) in Brazil brought major changes to be performed by corporations, especially how the companies store and process the collected data. Therefore, this article aims to show the risks for the companies that do not adapt to the LGPD, as well as the ways to comply to it, especially through efficient compliance programs. For this, a qualitative approach was used, with exploratory objectives, through

[1] Graduanda em Direito pela Universidade Tiradentes – UNIT. E-mail: annapaularnp@gmail.com

information collection procedures, mainly through bibliographic research and analysis of legislation. On the other hand, it was noticed that the risks of the non-adequation are potentially high and excessively harmful for the companies, making it necessary for them to adapt to the current legislation through programs such as compliance, which ensures furthering with the law and improves the risk management of the activity performed by the company.

Keywords: GDPL. Non-adequation. Compliance.

1 INTRODUÇÃO

Na era digital, inúmeras atividades são desenvolvidas em âmbito virtual, como transações financeiras, trabalho, estudo, relacionamentos sociais, comércio, o que torna a segurança dos dados transmitidos e armazenados pelas empresas uma preocupação constante.

Nessa nova era, vazamento e roubo de informações, venda de dados e até ataques cibernéticos tornaram-se cada vez mais comuns, colocando em risco a privacidade dos usuários. E muitos desses dados são tratados e compartilhados pelas empresas sem o consentimento de seus titulares, em clara violação ao direito à privacidade e a autodeterminação informativa.

Fora nesse cenário de invasão à privacidade dos usuários, ausência de consentimento no tratamento dos dados captados e *cibercrimes* que explodiu o número de escândalos envolvendo o vazamento de dados por grandes organizações, fazendo surgir uma nova tendência mundial: a necessidade de um regimento específico para a proteção de dados de seus titulares e também para que haja a devida responsabilização das empresas que violem tal legislação.

Assim como ocorreu na Europa, com a criação da *General Data Protection Regulation* (GDPR), que entrou em vigor em 2018 nos países da União Europeia, o Brasil, sob forte influência, sancionou a Lei nº 13.709 de 14 de agosto de 2018, denominada de Lei Geral de Proteção de Dados Pessoais (LGPD), trazendo uma série de disposições sobre o tratamento de dados pessoais, como as condutas a serem observadas pelas entidades públicas e privadas sob pena de incorrerem em sanções administrativas previstas em lei, cabendo, desse modo, a necessária adaptação destas entidades às novas exigências.

É nessa vertente e diante do grande impacto causado pela implementação LGPD no Brasil, em especial no setor privado, que o presente estudo se destina a mostrar a necessidade das organizações de estarem em conformidade com a nova legislação, através da implementação de eficientes programas de *compliance*, como forma tanto de prevenir riscos como também de maneiras de se voltar a legalidade, uma vez já tendo violado a referida legislação.

Dessa forma, questiona-se a importância da adoção de efetivas políticas de *compliance* à adaptação das organizações perante à LGPD, haja vista a previsão de responsabilização por parte das entidades que não estiverem em conformidade com a lei mediante a imposição de sanções administrativas.

Noutro giro, justifica-se esse trabalho pela atualidade do tema, sendo, por sua vez, uma tendência mundial à regulamentação do tratamento de dados pessoais, obrigando as empresas

a se adaptarem às novas regras, utilizando-se de programas de boa governança, como o *compliance*, com a finalidade de estarem em conformidade com a legislação, de reduzir custos, de evitar prejuízos e sanções administrativas como multas e o bloqueio dos dados que motivaram a infração.

Destaca-se que o presente estudo possui como objetivo geral expor a necessidade e os efeitos de programas como o *compliance*, para as organizações, em face da entrada em vigor da Lei Geral de Proteção de Dados. Além disso, objetiva-se trazer de forma breve a finalidade da lei; conceituar dados e identificar suas hipóteses de tratamento; apresentar a aplicabilidade da lei e suas exceções; apontar os riscos da não adequação à Lei, bem como ferramentas de adequação; conceituar o *compliance*, relacioná-lo com a Lei Geral de Proteção de Dados e dentro desse contexto demonstrar a importância do mesmo para as empresas.

A metodologia se baseou em um procedimento de coleta de informações através de pesquisas bibliográficas, legislação, artigos científicos e revisão de literatura, tendo uma abordagem qualitativa, haja vista a natureza da análise de conceitos e entendimentos de doutrinadores e pesquisadores, com objetivos exploratórios acerca do tema em estudo.

Este trabalho está dividido em cinco parte, sendo a primeira delas uma breve introdução do que será abordado ao longo do trabalho, contendo a contextualização e delimitação do tema, além dos objetivos e da metodologia abordada.

A segunda parte faz jus a conceituação de dados e tratamento de dados previstos na Lei de Proteção de Dados Pessoais, trazendo uma diferenciação dos tipos de dados, bem como a aplicabilidade e suas exceções da LGPD.

A terceira parte trata dos desafios impostos pela LGPD, como os riscos da não adequação a lei, a previsão de responsabilidade dos agentes e o ressarcimento de danos, e mostra também algumas das ferramentas existentes para que as empresas se adequem a nova lei.

A quarta parte discorre sobre o *compliance* e sua relação com a Lei Geral de Proteção de Dados, além dos requisitos mínimos de efetividade. Em seguida, traz a previsão das medidas de segurança da informação previstas em lei que devem ser observadas pelos programas de *compliance*.

Por fim, são apresentadas as considerações finais do trabalho após o estudo do tema proposto.

2 LEI GERAL DE PROTEÇÃO DE DADOS: CONCEITOS BÁSICOS E SUA APLICABILIDADE

2.1 Dados e Tratamentos de Dados à Luz da LGPD

Ao longo do tempo, a sociedade passou por diversas formas de organização social, de modo que, nos tempos atuais, possui a informação como seu principal elemento estruturante, em decorrência da impactante evolução tecnológica que fora capaz de criar mecanismos que transmitem e processam uma grande quantidade de informações em uma velocidade jamais vista (BIONI, 2019).

É nesse contexto da informação como elemento nuclear (BIONI, 2019), que milhares de dados são armazenados, transmitidos e processados, ou seja, tratados com as mais diversas finalidades, seja nas interações sociais ou em transações financeiras, motivando o surgimento de regulamentações de proteção de dados pessoais da pessoa natural, a fim de proteger, principalmente, o direito à privacidade e a autodeterminação informativa dos titulares dos dados, diante do fato de que a sociedade passou a ter cada vez mais dependência dos fluxos internacionais de bases de dados, principalmente relacionado às pessoas, uma vez viabilizados pelos avanços tecnológicos (PINHEIRO, 2020).

Conforme Patrícia Pinheiro (2020), a promulgação do Regulamento Geral de Proteção de Dados Pessoais (GDPR) na Europa acarretou em um "efeito dominó", haja vista que para manter relações comerciais com a União Europeia, os países e empresas deveriam ter uma legislação semelhante ao que previa a GDPR. Fora nesse cenário que no Brasil houve a publicação da Lei de nº 13.709 de agosto de 2018, denominada de Lei Geral de Proteção de Dados (LGPD).

Nessa vertente, a respeito da LGPD, a referida autora aduz que:

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis. (PINHEIRO, 2020, p.16)

Concluindo o entendimento anterior, Ana Frazão declara, ainda, que:

> a LGPD pretende regular todas as formas de tratamento de dados pessoais, que são definidos como quaisquer informações relacionadas a pessoa natural identificada ou identificável (art. 5º, I), incluindo até mesmo aqueles considerados públicos ou tornados públicos pelos titulares. (FRAZÃO, 2019, p.102)

Outrossim, para um melhor entendimento do presente estudo, torna-se mister compreender alguns dos conceitos básicos abordados no artigo 5º da LGPD, em especial no que tange aos dados, tendo em vista que a referida legislação traz a distinção entre dados pessoas, dados pessoais sensíveis e os dados anonimizados:

> Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

À vista disso, é possível observar que no tocante aos dados pessoais prevalece o conceito expansionista, em razão do fato de que um dado pessoal equipara-se a uma informação que identifica um sujeito, seja de maneira direta ou indireta, ou seja, abrange até as informações que possuem o potencial, ainda que remoto, de identificar um indivíduo (BIONI, 2019), como por exemplo idade, perfis de compras, dados de localização, dados acadêmicos, números de IP, entre outros (PINHEIRO, 2020).

Já em relação aos dados pessoais sensíveis, nos quais recebem uma proteção diferenciada, conforme Bruno Bioni (2019, p. 118), esses nada mais são que "uma espécie de dados pessoais que compreendem uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação." Nessa perspectiva, observa-se que dados pessoais sensíveis "são dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política", entre outros (PINHERIO, 2020, p. 36).

Agora, no que concerne aos dados anonimizados, a própria LGPD, em seu artigo 12, afirma que, em regra, esse tipo de dado não é considerado um dado pessoal para os fins de proteção da Lei, haja vista a incapacidade de identificar seu titular, ressalvando-se os casos em que o processo de anonimização for revertido.

Por outro lado, no tocante ao tratamento desses dados, o artigo 5º, inciso X da LGPD traz o seguinte conceito:

> 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;

Nota-se que a LGPD traz um rol meramente exemplificativo em relação ao tratamento de dados pessoais, sendo esse também orientado por princípios básicos previstos no artigo 6º da lei, como: boa-fé, finalidade, adequação (em que deve haver a compatibilidade do tratamento com as finalidades comunicadas ao titular dos dados), necessidade do tratamento, livre acesso (que é a garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento), segurança dos dados, transparência aos titulares, prestação de contas e responsabilização.

No mais, destaca-se as hipóteses previstas na LGPD para o tratamento de dados pessoais (artigo 7º) e dados pessoais sensíveis (artigo 11) a serem observadas pelas empresas.

Em referência ao tratamento de dados pessoais, o artigo 7º traz as seguintes hipóteses em que poderá haver tratamento:

> I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem); VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Já as hipóteses de tratamento dos dados pessoais sensíveis, a LGPD aponta, em seu artigo 11, que só poderá ocorrer quando o titular dos dados ou seu responsável legal consentir

de forma específica e para determinadas finalidades. Entretanto, poderá ocorrer também sem o consentimento do titular quando, por exemplo, do cumprimento de alguma obrigação legal, do exercício regular de direitos, para proteção da vida, entre outros.

Por fim, cabe observar também que o término do tratamento desses dados ocorrerá quando do fim do período previsto de tratamento, ou ainda no momento que for verificado que a finalidade fora alcançada ou que os dados deixaram de ser necessários para o alcance desta finalidade, ou quando do exercício do direito do titular para revogação do consentimento e por determinação da autoridade nacional, hipóteses essas previstas no artigo 15 da legislação em comento.

2.2 Aplicabilidade da Lei e suas Exceções

De acordo com a previsão do artigo 3º da LGPD, a lei será aplicada a qualquer operação de tratamento de dados pessoais realizada por organizações públicas ou privadas, por pessoa natural ou jurídica, independentemente do meio (físico ou virtual), do país de sua sede ou ainda do país em que estejam localizados os dados objeto de tratamento, e desde que envolva pelo menos um dos seguintes requisitos previsto no artigo supracitado:

> I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Nota-se, desse modo, que a Lei Geral de Proteção de Dados "não está relacionada à cidadania ou à nacionalidade dos dados pessoais, tampouco à residência do indivíduo titular" (PINHEIRO, 2020, p.39), mas sim a origem da coleta dos dados, ao local de seu tratamento, ou ainda quando a atividade que envolve o tratamento de dados tenha por objetivo ofertar ou oferecer bens ou serviços em território nacional. Por exemplo, "havendo um estrangeiro no Brasil, mesmo em trânsito, será protegido pela legislação brasileira no que se refere à operação com dados pessoais" (KOEPSEL, 2020, p. 21).

Em contrapartida, consoante previsão do artigo 4º, incisos I a IV, a referida legislação não será aplicada quando o tratamento de dados pessoais for realizado por pessoa física para fins particulares e não econômicos, ou seja, uso pessoal, para propósitos puramente jornalísticos ou artísticos, ou ainda acadêmicos, para finalidades relativas à segurança pública, defesa nacional, atividades de investigação e repressão a infrações penais, sendo que nesses dois

últimos, segundo GARCIA e colaboradores (2020), deverá haver legislação específica a respeito do assunto, além do fato de que o banco de dados não poderá ser utilizado por empresa privada.

Cabe ressaltar que em relação a não aplicabilidade da LGPD, no tocante a finalidade puramente acadêmica, o legislador relacionou a presente hipótese aos artigos 7º e 11 da própria LGPD, no que diz respeito aos requisitos de tratamento de dados pessoas e aos dados pessoais sensíveis, demonstrando a aplicação reduzida da presente hipótese, conforme entendimento de Cots e Oliveira (2019, apud KOEPSEL, 2020, p. 24):

> O Legislador, ao nosso ver, havia pretendido conter o ímpeto da iniciativa privada, que poderia se dedicar ao tratamento de dados pessoais sob o manto da produção acadêmica, mas com finalidades meramente comerciais. Um bom exemplo poderia ser estudos acadêmicos relativos ao desenvolvimento de novos medicamentos ou técnicas em saúde, com formação de banco de dados pessoais que poderia ser utilizado, indevidamente, em detrimento dos titulares.

Ademais, em conformidade com o que fora alegado, diante das hipóteses de aplicabilidade da LGPD e suas exceções legais, a imprescindibilidade da aplicação desta lei decorre da forma como está amparada a economia vigente, tendo em vista que a informação, hoje, é o principal elemento que estrutura a sociedade, funcionando como moeda de troca utilizada por usuários, seja pessoa física ou jurídica, empresa pública ou privada, para ter acesso a serviços, bens ou ainda conveniências (PINHEIRO, 2020).

Portanto, torna-se indispensável que as organizações públicas, e em especial as privadas, atentem-se às hipóteses de aplicabilidade da Lei Geral de Proteção de Dados, considerando os riscos que podem sofrer diante de sua não observância.

3 OS DESAFIOS IMPOSTOS PELA LGPD ÀS EMPRESAS E MEIOS DE ADEQUAÇÃO

3.1 Riscos da Não Adequação à Lei: a Previsão de Responsabilidade, o Ressarcimento de Danos e da Imposição de Sanções Administrativas

Com o intuito de tutelar a privacidade dos usuários de maneira eficaz através da proteção dos dados pessoais das pessoas físicas, em atenção a coleta, armazenamento, tratamento e a transferência segura desses dados, a Lei Geral de Proteção de Dados impôs severas punições

para quem descumprir suas determinações, especificando os envolvidos no processo de tratamento de dados para a devida responsabilização desses atores, assim como suas atribuições, responsabilidades e eventuais sanções a serem impostas, não restringindo, entretanto, sua aplicabilidade às empresas de tratamentos de dados (RODRIGUES, 2021).

> Ao contrário do que parece, a LGPD não se aplica apenas a empresas do segmento de tecnologia, mas a qualquer uma, tanto no setor público quanto no privado, que colete dados de seus usuários. Isso quer dizer que instituições bancários, cadastros de condomínio e até algumas páginas do Facebook deverão se adequar à nova lei de proteção de dados caso não queiram sofrer as sanções (SILVA, 2020 apud RODRIGUES, 2021, p. 58).

Nessa vertente, é válido compreender os conceitos de controlador e operador trazidos nos incisos do artigo 5º da LGPD, para saber a quem caberá a responsabilidade do tratamento de dados e o ressarcimento dos danos em casos de violação à lei:

> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; IX - agentes de tratamento: o controlador e o operador;

Observando o que dispõe a lei, nota-se que enquanto que as decisões relativas ao tratamento de dados cabem ao controlador, pessoa física ou jurídica, é o operador que propriamente realiza o referido tratamento a mando do primeiro, ou seja, ambos são os agentes de tratamento dos dados.

No que tange a responsabilização por violação à lei, tanto o operador como o controlador podem ser responsabilizados solidariamente quando causarem a outrem algum dano patrimonial, moral, individual ou coletivo, sendo obrigados a repará-lo, essa é a previsão do artigo 42 da LGPD:

> 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.

Inclusive, caso esses agentes de tratamento violem as normas definidas em lei, eles ficam sujeitos a sanções administrativas que podem variar desde uma pequena advertência até a pagamentos de multas em valores significativos, que podem acarretar até mesmo no fim de uma atividade empresarial, particularmente em relação às empresas de pequeno porte, caso sofram sucessivos vazamentos de dados pessoais (RODRIGUES, 2021).

Nessa conjuntura, a Lei Geral de Proteção de Dados elenca um rol, no artigo 52, de sanções administrativas que podem ser aplicadas em decorrência do descumprimento da referida legislação, obviamente para serem aplicadas apenas após um procedimento administrativos que permita a ampla defesa (§1º), devendo ainda serem observados critérios que vão desde a gravidade e a natureza das infrações e dos direitos pessoais afetados até a adoção de política de boas práticas e governança, parâmetros situados respectivamente nos incisos I e IX do §2º do supramencionado artigo.

Há a previsão das seguintes penalidades estabelecidas no artigo 52, caput:

> I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração;
> [...]
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Isto posto, em que pese o prejuízo que essas sanções possam causar às empresas que descumprirem a lei, elas são, de fato, indispensáveis para uma tutela eficaz de proteção de dados (RODRIGUES, 2021). Ademais, nota-se também que a implementação de um eficiente programa de gestão de dados pessoais cumulada com uma política de boas práticas e governança podem ajudar as empresas na redução dessas penas estipuladas, quando da ocorrência de alguma infração (PINHEIRO, 2019).

Por outro lado, não são só os riscos trazidos pelas sanções previstas na LGPD que as empresas devem temer. A não adequação com a legislação em comento pode dar pretexto para

que se instaure um ambiente de instabilidade dentro das organizações, diante da ausência de recursos de um controle adequado sobre os dados tratados e de padrões éticos, que podem dar ensejo à prática de atos ilícitos, o que, consequentemente, acaba por prejudicar a imagem da empresa e enfraquece sua colocação no mercado, dificultando seu relacionamento com outras empresas (NÓBREGA; ARAÚJO, 2019).

Dessa forma, tendo como pressuposto que muitas entidades estão cada vez mais empenhadas e preocupadas em adotar políticas de adequação às leis, ou seja, programas de conformidade, pode ter um custo altíssimo contratar uma empresa que possua má reputação no que concerne à preocupação com o atendimento às leis, podendo levar a interrupções de negociações e, inclusive, ao encerramento de acordos já existentes (NÓBREGA; ARAÚJO, 2019).

Por isso, consoante alega Rodrigues (2021, p. 61), a instauração de "procedimentos aptos a colocar em conformidade a atividade empresarial nos ditames da LGPD é essencial para o fortalecimento da atividade econômica e da própria sobrevivência da empresa em um mercado cada vez mais competitivo."

3.2 Ferramentas de Adequação como Forma de Prevenção de Riscos

Consoante alerta Rodrigues (2021), o advento da Lei Geral de Proteção de Dados trouxe grandes impactos socioeconômicos e tornou cada vez mais importante que as empresas, públicas ou privadas, tenham o domínio da gestão dos dados captados. Fora nesse cenário que surgiram mecanismos que auxiliam no gerenciamento de informações, no controle de riscos e na correta adequação com a lei, como o gerenciamento de riscos, o mapeamento de dados, as boas práticas de governança e, em especial, o *compliance*.

Em relação ao gerenciamento de riscos, o Instituto Brasileiro de Governança Corporativa (2017) traz o entendimento de que tal ferramenta está contida no planejamento de negócios das empresas através de um sistema pensado para identificar os eventos que ocasionam riscos aos objetivos da corporação e para responder a essas ocorrências de forma eficiente mantendo o pleno funcionamento da organização, reduzindo, por conseguinte, a probabilidade e o impacto de possíveis perdas. Assim, a ausência desse instituto, ou ainda sua má aplicação acarretam em consequências negativas que acabam por colocar em risco o desenvolvimento da empresa.

Entretanto, esse modelo exige alto investimento econômico que envolve tanto a captação e o armazenamento, como o processamento das informações e a grande quantidade de pessoas necessárias à formação de equipes multidisciplinares para que seja feita uma gestão de riscos eficiente (NEVES; FIGUEIROA, 2019).

O mapeamento de dados, por sua vez, também chamado de *data mapping*, nada mais é do que um documento que demonstra o processo e o método em que fora submetido os dados pessoais dos usuários, o que engloba os procedimentos pelos quais os dados transitam desde sua origem, o nível de segurança da base de dados no qual o dado está inserido, como e com quem eles são compartilhados e onde estão armazenados, o que acaba por permitir que a empresa possua uma ampla visão de como ela lida com o processo de gestão desses dados (RODRIGUES, 2021).

No tocante às boas práticas e governança, é essencial para a efetivação das exigências previstas em lei, envolvendo procedimentos de reeducação, adequação e prevenção, treinamentos em prol da segurança dos dados tratados (PINHEIRO, 2019). Tal ferramenta, se preocupa com as questões operacionais do procedimento de tratamento de dados, definindo os padrões técnicos que irão estruturar todo o sistema de tratamento (FRAZÃO; OLIVA, ABILIO, 2019).

Cabe ressaltar que no artigo 50 da Lei Geral de Proteção de Dados há a previsão expressa das boas práticas e das condutas de governança, permitindo que as empresas que realizam o tratamento de dados definam, por exemplo, as condições de organização, o regime de funcionamento, as normas de segurança, os padrões técnicos, entre outros aspectos, contribuindo na construção de uma boa reputação e se destacando no mercado em que atuam (RODRIGUES, 2021).

Por fim, uma das mais importantes, completas e eficientes ferramentas de adequação à lei, o *compliance*. Esse método, faz parte de um processo bem organizado, mas ao mesmo tempo complexo que compreende mecanismos de conservação de valores, objetivos e princípios de uma empresa, além do controle de riscos, fazendo parte da estratégia de desenvolvimento da organização, o que acaba por gerar um ambiente de segurança jurídica e confiabilidade no ramo em que se atua (BERTOCCELLI, 2019), sendo um dos melhores programas de conformidade que uma empresa pode adotar diante dos riscos advindos com a implementação da LGPD.

4 ADEQUAÇÃO DA LGPD ATRAVÉS DOS PROGRAMAS DE *COMPLIANCE*

4.1 Conceito e Requisitos Mínimos de Efetividade

Rodrigo de Pinho Bertoccelli (2019) discorre que a palavra c*ompliance* tem sua origem no verbo inglês *to comply,* que nada mais é do que estar em conformidade, seja com a lei ou ainda com o regimento interno de uma empresa e seus padrões éticos, servindo de ferramenta para prevenção e redução de riscos, preservando o desenvolvimento saudável da corporação, estando esta ferramenta de adequação intimamente ligada a boa governança de uma empresa.

Dessa maneira, o *compliance* envolve uma série de esforços com a finalidade de fazer com que a empresa e todo seu corpo de funcionários, inclusive o alto escalão da corporação, adotem comportamentos desejáveis e adequados com os princípios éticos e objetivos da empresa (ARTESE, 2019).

A implementação de programas de *compliance* em observância à nova lei brasileira de proteção de dados pessoais é uma das melhores e mais completas ferramentas de adequação à legislação e traz vantagens àqueles que a implementam, tendo em vista que permite a adequada gestão de riscos da atividade desenvolvida pela corporação, impulsiona a criação de uma cultura organizacional de observância às normas legais, viabiliza a identificação de ocasional descumprimento e ajuda a minorar eventuais prejuízos (FRAZÃO; OLIVA; ABILIO, 2019).

Ademais, cabe salientar que a instalação desses programas de integridade servem também como atenuante no caso de punições administrativas, sendo levadas em consideração na aplicação das sanções previstas na LGPD, conforme os seguintes incisos do artigo 52, §1º da mencionada legislação:

> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> [...]
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei; IX - a adoção de política de boas práticas e governança; X - a pronta adoção de medidas corretivas;

Por outro lado, torna-se imprescindível a existência de alguns requisitos mínimos para a eficiente implementação do programa de *compliance*.

O primeiro requisito é a avaliação periódica dos riscos a que uma empresa se submete através da identificação dos pontos vulneráveis e atualização do programa de conformidade de

acordo com a necessidade que surge na corporação durante sua atuação no mercado. O referido elemento objetiva identificar de forma antecipada as áreas da empresa que estão expostas a riscos para que, assim, sejam adotadas medidas preventivas (FRAZÃO; OLIVA; ABILIO, 2019), estando esse primeiro requisito previsto na LGPD no artigo 50, §2º, inciso I, alínea h, que trata das condutas que devem, no mínimo, ser implementadas por programas de governança/conformidade.

Outro elemento importante é a elaboração de um Código de Ética e de Conduta com a finalidade de listar de forma detalhada os procedimentos que a pessoa jurídica deve adotar no tratamento de dados, explicitando desde os dados que poderão ser coletados e tratados, para quais finalidades e em quais hipóteses (FRAZÃO; OLIVA; ABILIO, 2019).

O estabelecimento de uma organização interna compatível com o risco da atividade exercida pela empresa em relação ao tratamento dos dados coletados, o comprometimento da alta administração e um setor de *compliance* autônomo e independente são também requisitos essenciais para o êxito do programa de *compliance* (FRAZÃO; OLIVA; ABILIO, 2019).

Se faz necessário também tanto o fornecimento de um treinamento adequado aos funcionários da empresa a respeito das técnicas a serem adotadas para a proteção dos dados pessoais, como também a adoção de uma tecnologia que proporcione um eficaz cumprimento das normas, além do monitoramento constante do controle dos dados para a detecção rápida de ilegalidades que possam surgir e a criação de uma cultura corporativa que respeite a legislação, assim como a apuração e punição das condutas que forem contrárias ao programa implementado (FRAZÃO; OLIVA; ABILIO, 2019).

Isto posto, ressalta-se que a implementação de um programa de integridade envolve um alto investimento financeiro diante do dispêndio de recursos a serem utilizados para a eficácia desta ferramenta, como para a criação de códigos de ética, estruturas de controle e fiscalização e treinamento de profissionais, entre outros. Entretanto, os custos de não estar em conformidade com a nova lei de proteção de dados são consideráveis e potencialmente muito altos, podendo superar os gastos com a implementação do programa de *compliance* diante das sanções administrativas previstas na LGPD e o enfraquecimento da imagem da empresa perante o mercado (NÓBREGA; ARAÚJO, 2019).

4.2 Políticas de *compliance* utilizadas como artifício de defesa das organizações diante da previsão das medidas de segurança previstas na Lei nº 13.709, de 14 agosto de 2018

Em atenção aos requisitos necessários à eficácia dos programas de *compliance*, esses devem se atentar às medidas de segurança e sigilo de dados previstos na primeira seção do capítulo VII da LGPD.

O programa de conformidade deve promover a segurança da informação armazenada e tratada, assegurando a integralidade e a confiabilidade de todos os tipos de dados e ao longo de todo o caminho trilhado pelo dado dentro dos sistemas das empresas, devendo o programa ser usado como forma de defesa dentro das corporações, em decorrência dos riscos a que são expostas com a entrada em vigor da LGPD (PINHEIRO, 2019).

Por isso, ressalta-se que para seja garantida a proteção dos dados, bem como o correto tratamento dos mesmos, cabe aos agentes que são responsáveis por esse processo, ou pessoa que de alguma forma intervenha em alguma de suas fases, a adoção de medidas de segurança satisfatórias ao risco exposto pela atividade (PINHEIRO, 2019).

A Lei Geral de proteção de Dados traz a previsão, no artigo 46, caput, da adoção das medidas de segurança no tratamento dos dados, salientando, em seguida, que tais medidas deverão ser consideradas desde a fase de concepção do produto ou serviço, ou seja, desde o início, até sua a execução.

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
> [...]
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Frisa-se que a Autoridade Nacional de Proteção de Dados (ANPD), uma espécie de agência reguladora, também poderá dispor a respeito dos padrões técnicos mínimos a serem adotados pelos agentes de tratamento para a segurança dos dados, de forma que será levado em consideração a natureza das informações tratadas, as características do tratamento dos dados, o estado da tecnologia, em especial no tocante aos dados pessoais sensíveis, bem como os princípios previstos em lei, conforme dispõe o §1º do artigo 46 da LGPD.

Diante de qualquer incidente de segurança que acarrete riscos ou ainda danos aos titulares dos dados, como vazamento de informações, é dever do controlador, um dos agentes de tratamento, comunicar à ANPD sobre o ocorrido e em um prazo razoável a ser definido pela própria autoridade, que irá verificar a gravidade da situação, podendo determinar a adoção de providências a serem tomadas pelo controlador, como a aplicação de medidas para reverter ou

minimizar os danos e a divulgação do incidente em meios de comunicação, consoante previsão do artigo 48, caput e §2º da LGPD.

As corporações devem se atentar que a comunicação à ANPD deverá mencionar, no mínimo, os requisitos estabelecidos nos incisos do §1° do artigo 48:

> I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Por fim, observa-se que um programa de *compliance* voltado para adequação da LGPD nas corporações auxilia a aplicação eficaz das normas previstas em lei pelos agentes de tratamento, como as medidas de segurança, minimizando incidentes que ocasionam prejuízos à empresa, mitigando riscos, estabelecendo uma relação de confiabilidade com os titulares dos dados (FRAZÃO; OLIVA; ABILIO, 2019), ao passo que transmite segurança, fortalece a colocação da empresa no mercado e instaura um ambiente de estabilidade na corporação (NÓBREGA; ARAÚJO, 2019).

5 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados (LGPD) surgiu no Brasil com a finalidade de proteger os dados pessoais e os dados pessoais sensíveis dos usuários em uma sociedade que possui a informação como seu principal elemento estruturante, tutelando princípios e direitos, e em especial o direito à privacidade e a autodeterminação informativa.

Entrementes, a LGPD também trouxe enormes mudanças e desafios às empresas, que para não ficarem na ilegalidade, precisam se adequar às normas previstas em lei, tendo em vista os riscos a que ficam expostas como a estipulação de severas penalidades aqueles que não estiverem em conformidade, a devida responsabilização dos infratores e o ressarcimento dos eventuais danos causados aos titulares dos dados.

É nesse cenário de desafios advindos com a entrada em vigor da LGPD, que as empresas necessitam buscar ferramentas que possibilitem o controle seguro dos dados captados e tratados, bem como uma mudanças nos padrões éticos e de segurança de dados, e dentre as

várias ferramentas existentes, existe o *compliance*, uma das mais completas e eficientes formas de adequação à lei.

A partir disso, a implementação de um eficiente programa de *compliance*, fundado em requisitos como avaliação de riscos, elaboração de um código de conduta, comprometimento da alta administração, treinamento de equipe, entre outros, torna-se essencial para que as empresas estejam em conformidade com a legislação vigente, pois minimiza prejuízos, cria uma cultura corporativa de observância à lei, uma melhor gestão de riscos da atividade, além de fortalecer a atividade econômica da corporação em um mercado competitivo.

REFERÊNCIAS

ARTESE, Gustavo. Compliance Digital: Proteção de Dados Pessoais. In: CARVALHO, André Castro et al (Coord.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019.

BERTOCCELLI, Rodrigo de Pinho. Compliance. In: CARVALHO, André Castro et al (Coord.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais:** A função e os limites do consentimento. Rio de Janeiro: Editora Forense, 2019.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 outubro 2020.

FRAZÃO, Ana; Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. cap.4, p. 99-129.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Viviane da Silveira. Compliance de dados pessoais. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro.** São Paulo: Thomson Reuters Brasil, 2019. cap.10 p. 677-715.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: guia de implantação. São Paulo: Blucher, 2020.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de riscos corporativos:** evolução em governança e estratégia**.** Série Cadernos de Governança Corporativa – 19. São Paulo: IBGC, 2017.

KOEPSEL, Alice de Medeiros. **Adoção e Efeitos dos Programas de Compliance à Luz da Lei Geral de Proteção de Dados Pessoais**. Monografia (Graduação em Direito) – Universidade do Sul de Santa Catarina. Tubarão. 2020. Disponível em:

https://riuni.unisul.br/bitstream/handle/12345/9626/MONOGRAFIA%20-%20ALICE%20KOEPSEL.pdf?sequence=1&isAllowed=y. Acesso em: 21 set. 2020.

NEVES, Edmo Colnaghi; FIGUEIROA, Caio Cesar. Gestão de Riscos. In: CARVALHO, André Castro et al (Coord.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019.

NÓBREGA, Marcos; ARAÚJO, Leonardo Barros C. de Araújo. Custos do Não Compliance. In CARVALHO, André Castro et al (Coord.). **Manual de Compliance**. Rio de Janeiro: Forense, 2019.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2020.

RODRIGUES, Tatiana Kolly Wasilewski. Lei Geral de Proteção de Dados (LGPD) e Data Mapping (Mapeamento de Dados): Desafios, Perspectivas e como se Adequar à Nova Lei na Prática. In: TEIXEIRA, Tarcisio (Coord.). **Empresas e Implementação da LGPD – Lei Geral de Proteção de Dados Pessoais.** Salvador: Editora JusPodivm, 2021, cap. 2, p. 51-73.