OS PROGRAMAS DE COMPLIANCE E A ADOÇÃO DA PROTEÇÃO DE DADOS PESSOAIS À LUZ DA LGPD.

July Samary dos Santos Araujo e Marco Aurélio Pinto Florêncio Filho

Apoio:PIVIC Mackenzie

RESUMO

O contexto dessa temática se constitui em meio as discussões, repercussões nacionais e internacionais impulsionadas pela Lei Geral de Proteção de Dados (LGPD) em um dos períodos de circulação latente de informações no mundo digital e, inevitavelmente, de alta escala de dados pessoais. Nesse sentido, propõe-se uma análise no âmbito da iniciativa privada, sugerindo maneiras para que as empresas lidem com esse processo de adequação e adoção às boas práticas e normas de *compliance* à luz da LGPD, haja vista que as fiscalizações e as sanções previstas passaram a ocorrer a partir de 1º de agosto de 2021 sob a ação da Autoridade Nacional de Proteção de Dados (ANPD). O presente trabalho expõe, a partir de um ponto de vista crítico, quais são os impactos nos programas de *compliance* em proteção de dados pessoais; enquanto instrumentos de mitigação de risco, e quais são as consequências de sua não adequação. Além de promover a reflexão acerca dos programas de *compliance* – enquanto mecanismos centrais – no processo de implementação da LGPD às instituições que tratam dados pessoais. Para tanto, utiliza-se o método científico qualitativo, fundamentado em estudos doutrinários e legal.

PALAVRAS-CHAVE: Adequação. Programa de *compliance*. LGPD.

ABSTRACT: The context of this theme is constituted amidst the discussions, national and international repercussions driven by the General Data Protection Law (LGPD) in one of the periods of latent circulation of information in the digital world and, inevitably, of a high scale of personal data. In this sense, an analysis within the private sector is proposed, suggesting ways for companies to deal with this process of adaptation and adoption of good practices and compliance standards in the light of the LGPD, given that the inspections and sanctions provided for have passed to take place from August 1, 2021 under the action of the National Data Protection Authority (ANPD). The present work exposes, from a critical point of view, what are the impacts on compliance programs in the protection of personal data; as risk mitigation instruments, and what are the consequences of their inadequacy. In addition to promoting reflection on compliance programs – as central mechanisms – in the process of implementing the LGPD to institutions that process personal data. Therefore, the qualitative scientific method is used, based on doctrinal and legal studies.

KEYWORDS Adequacy. Compliance program. LGPD.

1. INTRODUÇÃO

Após adiamentos e discussões, a Lei nº 13.709/2018, conhecida como LGPD, foi sancionada em agosto de 2018 e entrou em vigor, efetivamente em 18 de setembro de 2020. A LGPD dispõe acerca de medidas para o tratamento de dados pessoais. Vale mencionar que, antes de sua sanção, havia leis setoriais esparsas e de aplicação difusa, por exemplo, a Lei de Sigilo Bancário (Lei Complementar nº 105, de 10 de janeiro de 2001), a Lei do Cadastro Positivo (Lei nº 12.414, de 9 de junho de 2011), o Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990) e o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014). Dessa maneira, é importante ressaltar que, quando elaborado, o projeto de pesquisa se propunha a analisar os programas de c*ompliance* enquanto precursores na proteção de dados pessoais, uma vez que a LGPD ainda não estava em vigor e havia um Projeto de Lei (PL nº 11.79/20) em andamento que poderia alterar sua vigência, para maio de 2021, o qual não logrou êxito. Sendo assim, a análise foi feita de uma perspectiva de efetividade e da adoção das novas diretrizes nos programas de *compliance* à luz da LGPD.

Com esse marco normativo, a LGPD passou a abranger todas as situações que envolvam o tratamento de dados pessoais, tendo sido impulsionada, principalmente, por fatores provenientes no âmbito internacional (MENEZES; COLAÇO, 2019, p. 161), tal qual a entrada em vigor do regulamento europeu, além das constantes notícias na mídia envolvendo vazamentos e má utilização dos dados. Além disso, propício mencionar o caso que ganhou repercussão mundial, relacionado às infrações cometidas pela empresa Cambridge Analytica, acusada de manipular os dados pessoais de mais de 50 milhões de usuários da rede social Facebook. Baseando-se em dados coletados do aplicativo móvel, a empresa foi capaz de realizar um estudo comportamental de seus usuários, chegando a prever suas possíveis ações e tomadas de decisões, ocasionando a interferência das eleições de 2016 dos EUA e no BrexiT (G1, 2018).

Destarte, a LGPD se destina a todas as pessoas naturais ou jurídicas, de direito público ou privado que tratem dados pessoais. Segundo o art. 5º, X da LGPD, o tratamento de dados pessoais é entendido como toda operação realizada coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Surge ainda, a necessidade de autorregulação, especialmente no que diz respeito à seção II da LGPD, intitulada “Das Boas Práticas e da Governança”. Em obra relativa a comentários à LGPD, Jimene (2021, p. RL-14 – RL-1.15), assevera sobre o artigo 50, primeiro artigo da referida seção:

> [...] fica claro que a LGPD está imbuída de forte viés de governança corporativa, estimulando a implementação de um Programa de Governança em Privacidade, que estabeleça controles internos para gestão do tema a fim de viabilizar a conformidade com a legislação, o qual nada mais é do que um programa de *compliance*. É a partir desse Programa de Governança que serão definidas e documentadas as medidas adotadas pela entidade para o respeito à lei.

Em vista disso, o objetivo desta pesquisa foi justamente analisar o papel que programas de *compliance* desempenham na proteção de dados pessoais enquanto principal ferramenta de adoção à LGPD, e demonstrar a importância prática de as instituições sujeitas à LGPD reverem constantemente seus mecanismos internos de governança corporativa, considerando a relevância do tema nos dias atuais e a necessidade de ter uma boa reputação no mercado que tem se mostrado cada vez mais exigente e intolerante com instituições que se dizem aderentes à uma norma ou até mesmo à uma causa e na sequência, expõe-se um evidente descumprimento, demonstrando-se a falta de aderência.

Nesse sentido, a exemplo, pode-se citar, o caso recente envolvendo a Amazon que recebeu multa recorde da União Europeia, no montante de US$ 887 milhões que representa 0,2% da receita total da companhia, avaliada em 386 bilhões de dólares, por motivos de violações à lei de proteção de dados europeia, que em muito influenciou a LGPD.[1] Considerando esse cenário, é essencial que medidas voltadas às boas práticas e governança sejam estendidas à proteção de dados pessoais e, desse modo, surge a necessidade de se compreender a relevância que programas de *compliance* assumem na tutela da proteção dos dados pessoais e no direcionamento dos agentes de tratamento a respeito das condutas fundamentais para atender aos preceitos legais, bem como compreender as disposições que devem ser observadas no que se refere à LGPD.

2. O PROGRAMA DE *COMPLIANCE* ENQUANTO MECANISMO DE EFETIVAÇÃO E ADOÇÃO DA LGPD

Antes de realizar tal correlação, primeiro, é essencial que seja traçado um paralelo entre os programas *compliance* e a LGPD, regressando a alguns aspectos centrais do *Compliance* propriamente dito.

Compliance é um termo originado da língua inglesa "*to comply*" que pode ser traduzido como "conformidade". A definição técnica do *U.S Federal Sentencing Guidelines Manual*

[1] PANCINI, Laura. Amazon recebe multa recorde de US$ 887 milhões da União Europeia. **EXAME.** 30 jul. 2021. Disponível em: <https://exame.com/tecnologia/amazon-multa-recorde-da-uniao-europeia/> Acesso em: 02 set. 2021.

(2018, p. 10) que traduzido pode ser entendido como “Manual de Diretrizes de Sentenciamento Federal dos EUA” estabelece que *compliance* é o “dever das empresas de promover uma cultura organizacional que estimule a conduta ética e um compromisso com o cumprimento da lei”.

Em suma, há o entendimento de que o *compliance* é o cumprimento das normas, tanto as leis de um país, quanto às diretrizes internas de uma empresa, instituição de ensino, associação de classe entre outros. Pode trazer o sentido de: “ser ético e transparente”. O termo vem sendo utilizado ainda como sinônimo de integridade.

Para o Conselho Administrativo de Defesa Econômica (CADE), “*compliance* é um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores” (BRASIL, 2016, p. 9).

Para garantir o efetivo cumprimento das normas fixadas nos programas de *compliance*, afigura-se – igualmente – necessário estabelecer uma organização com procedimentos e controles internos compatíveis com as avaliações de riscos. Nesse contorno, há a preocupação em implementar as reestruturações necessárias ao atendimento dos perigos identificados, inclusive estabelecendo um setor independente e com recursos para exercer a função de vigilância e assegurar o respeito ao programa, além de representar importante padrão de conduta dos próprios administradores (FRAZÃO, 2017).

No âmbito da proteção de dados pessoais, tem-se mais um mecanismo de gestão de riscos e conforme leciona Moraes (2020, p. 546-547):

> Já os programas de *compliance,* como instrumento de governança corporativa, talvez sejam a melhor forma de as organizações se adequarem a estas regulamentações, sejam elas relacionadas à anticorrupção, prevenção à lavagem de dinheiro, antitruste ou, no caso em tela, proteção de dados pessoais e privacidade. Vale lembrar que, conceitualmente, programas de *compliance* são conjuntos de medidas adotadas e asseguradas pelos agentes de governança para que as organizações estejam em conformidade com seus princípios e valores, mas também com as leis e regulações às quais estão submetidas.

Há quem defenda, inclusive, que um programa de integridade não é um programa de *compliance*. Em linhas gerais, seria atribuído ao programa de integridade corporativa uma função de caráter essencialmente ético e moral; enquanto o Programa de *Compliance*, poderia ser classificado como uma modalidade de monitoramento, destinado a verificar se as diretrizes estão sendo cumpridas de acordo com os procedimentos estabelecidos. Logo, não podem ser tratados como sinônimos, pois se uma empresa não possui um programa de integridade corporativa enraizado em sua cultura, dificilmente, obteria sucesso na implementação de um Programa de *Compliance,* para fins de monitoramento (BARCAT,

2017). Feita tal ponderação, seguiremos neste trabalho, tratando aspectos oriundos aos programas de *compliance,* no âmbito da proteção aos dados pessoais.

Para que seja obtida a finalidade que se propõe um Programa de *Compliance* aplicado aos dados pessoais, é importante que se preze pela análise e gestão de riscos no tratamento de dados pessoais, e conforme asseveram pesquisadores em direito digital: “é preciso aplicar a prática de uma *gestão de riscos*, com a adoção de um conjunto de ações coordenadas, com o objetivo de controlar os possíveis impactos que um determinado tratamento pode gerar“ dando ênfase à necessidade de visibilidade e mapeamento de tratamento de dados pessoais, tanto por parte do controlador quanto do operador, que ressalte-se, podem vir a responder solidariamente, nos termos do artigo 42, § 1º, I da LGPD. À vista disso, de forma conservadora, entende-se por sinônimo de boas práticas que, ainda que a LGPD imponha o chamado: “registro das operações de tratamento de dados pessoais" (artigo 37, LGPD) apenas para algumas hipóteses legais; esse relatório contendo a descrição do processamento de dados pessoais pode ser realizado espontânea e voluntariamente como ferramenta de apoio e controle interno (OLIVEIRA; ABRUSIO; RONCAGLIA, 2021).

Nessa lógica, a LGPD orienta os controladores a inserirem as políticas de governança em privacidade em sua estrutura geral de *compliance*, com a previsão de mecanismos de supervisão internos e externos (art. 50, §2º, inciso I, f). Dessa forma, como bem esclarecem Frazão, Oliva e Abilio (2019, p. 36-37):

> [...] a indicação de membro da alta administração como responsável pelo setor de *compliance* (o *compliance officer* ou *chief compliance officer*), com atribuição para controlar e supervisionar o dia a dia do programa, o que inclui constante monitoramento e a implementação das políticas necessárias para garantir o sucesso do programa (com autonomia para tomar decisões e realizar investigações), consiste em elemento que confere robustez ao programa. Recomenda-se, ainda, que se garanta um canal de comunicação direto entre o *compliance officer* e os órgãos de administração da companhia e, sempre que possível, sua independência dos demais setores. Especificamente no que tange à LGPD caberá ao *compliance officer* garantir a observância dos parâmetros legais no tratamento de dados, buscando constante aprimoramento em segurança de dados, procurando manter a companhia conectada com os últimos desenvolvimentos tecnológicos do setor.

Ainda, o art. 50, § 2º, I, g da LGPD dispõe que o programa de governança em privacidade deve contar com “plano de resposta a incidentes e remediação”, isto é, deve antever mecanismos de detecção e remediação das condutas contrárias ao programa e a LGPD.

Ademais, o instrumento deve observar a comunicação tempestiva à Autoridade Nacional de Proteção de Dados (ANPD), conforme prescreve o art. 48 da LGPD nos casos

em que o incidente de segurança: “possa acarretar risco ou dano relevante aos titulares”, nos moldes requisitados pelo § 1º (BRASIL, 2018, p. 14):

> identificando a natureza dos dados, os titulares afetados, quais as medidas tomadas para a proteção dos dados, os riscos decorrentes do incidente, as medidas de reversão ou mitigação dos danos e, se for o caso, porque a comunicação não foi imediata.

Além de identificar a verificação de conduta de não conformidade, o programa deve também apresentar mecanismos de apuração dos responsáveis e sua adequada punição (FRAZÃO; OLIVA; ABILIO, 2019).

Nessa esteira, para um Programa de *Compliance* em proteção de dados, ou seja, adequado à LGPD, é possível se utilizar de algumas diretrizes contempladas no material elaborado pela Controladoria-Geral da União, denominado: “Programa de Integridade– Diretrizes para Empresas Privadas” (BRASIL, 2015, p. 10-25). O qual define o programa de integridade como: “um programa de *compliance* específico para prevenção, detecção e remediação dos atos lesivos previstos na lei nº 12.846/2013, que tem como foco, além da ocorrência de suborno, também fraudes nos processos de licitações e execução de contratos com o setor público” e estabelece os cinco pilares do Programa de Integridade, quais sejam: (i) comprometimento e apoio da alta direção; (ii) instância responsável pelo Integridade; (iii) análise de perfil e riscos; (iv) estruturação das regras e instrumentos; e (v) estratégias de monitoramento contínuo. A seguir, adentraremos em cada um dos referidos pilares, buscando a compreensão da relevância de sua aplicabilidade em programas de *compliance* em LGPD.

2.1. Comprometimento e Apoio da Alta Administração

O pilar que se refere ao Comprometimento e Apoio da Alta Administração possui amparo legal no art. 50 da LGPD, sendo reforçada tal relevância por estudos na área, mencionados anteriormente. Desta forma, considerando a influência que a liderança exerce sobre seus colaboradores, pode-se dizer que o comprometimento da alta administração é peça principal para a implementação de um programa de integridade robusto e efetivo. O também chamado de *“tone at the top/ tone from the top”* é o comprometimento demonstrado pelo alto escalão da empresa demonstrando que o exemplo vem do topo da cadeia de comando determinando uma cultura ética. Portanto, da mesma forma que para que um Programa de Integridade resulte em impactos positivos nas instituições, o mesmo entendimento é adotado em se tratando de um programa de *compliance* adequado à LGPD.

2.2. Instância responsável pelo Programa de Integridade

Os membros da alta direção devem adotar as medidas necessárias para definir uma instância interna independente responsável por desenvolver, aplicar e monitorar o Programa de Integridade. No âmbito de adoção de medidas relacionadas à LGPD, pode-se mencionar a figura do Encarregado de Proteção de Dados (*Data Protection Officer – DPO)*, em que a LGPD institui a obrigatoriedade para instituições que lidem com tratamento de dados em larga escala, excepcionando-se a hipótese de eventual dispensa da necessidade de sua indicação pela autoridade nacional "conforme natureza e o porte da entidade ou o volume de operações de tratamento de dados" nos termos do artigo 41§3º, e a quem devem ser dirigidas questões relacionadas a incidentes de eventuais violações e vazamentos, por exemplo.

Um Programa de *Compliance* em proteção de dados pessoais requer a alocação de recursos financeiros, materiais diversos e humanos adequados ao que se busca com o *compliance*, considerando que o ônus do não cumprimento é muito maior para as instituições, como veremos adiante. A instância interna, responsável, deve ter autonomia para exercer suas atividades e tomar decisões.

Ainda, deve ser assegurada condições para ministrar treinamentos, gerenciar o canal de denúncias da empresa e implementar outros procedimentos de monitoramento e controle, de modo a garantir o funcionamento do programa na prática.

O canal de denúncias é uma ferramenta importante na identificação de eventuais incidentes de segurança. Bandeira; Serraglio; Freire e Maluf (2020, p. 446) asseveram que:

> Um dos pilares essenciais de um programa de *compliance* é a existência de canal para recebimento de denúncias sobre descumprimento de leis e/ou de regras de conduta da empresa. Diferentes formatos podem ser adotados, sendo alguns canais abertos apenas ao público interno e outros abertos também ao público externo, permitindo-se, ou não, o anonimato do denunciante. O canal pode, ainda, ser administrado por equipe interna, com uso de ferramenta própria ou de plataforma contratada, ou totalmente administrado por consultoria externa à empresa.

Ainda, apontam que caso haja desdobramentos a partir do canal de denúncias, como uma investigação corporativa interna para apuração dos fatos, é importante assegurar o anonimato e sigilo. No âmbito da proteção de dados pessoais, as investigações corporativas podem ser amparadas pelo o legítimo interesse do controlador e a depender do caso concreto, poderão obter amparo no cumprimento de obrigação legal ou regulatória pelo controlador.

Ressaltam ainda que a prioridade é que os processos de investigação estejam alinhados aos princípios da LGPD, possuindo uma finalidade específica e propósitos

legítimos. Os dados coletados precisam ser realmente relevantes, em cumprimento ao princípio da qualidade, e não excessivos, atendendo ao princípio da necessidade.

2.3. ANÁLISE DE PERFIL E RISCOS DA INSTITUIÇÃO

O pilar que se refere a análise de perfil e riscos consiste nas características específicas da instituição, considerando setor de atuação, estrutura organizacional, quantidade de funcionários, terceiros contratados, grau de interação com a administração pública (de modo direto ou através de terceiros), e participação societária em outras empresas e/ou em consórcios.

Em se tratando da adoção de boas práticas voltadas à LGPD, é recomendável que sejam avaliados os riscos relacionados, principalmente, a terceiros contratados (pessoas jurídicas em sua maioria) que sejam controladoras ou operadoras, uma vez que causado o dano, a LGPD determina responsabilidade solidária entre controlares e operadores, conforme dispõe o 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.”

Por conseguinte, os riscos devem ser avaliados e mapeados considerando a possibilidade de ocorrência de algum evento que impacte nos valores e objetivos da instituição. Nesse mapeamento, deverá haver a determinação da base legal e a finalidade para cada tratamento, além de todo o ciclo de vida dos dados, para enfatizar a cautela com a informação: coleta, processamento, análise, compartilhamento, armazenamento, reutilização e eliminação.

Vale sublinhar a importância fundamental de que: i) haja revisão das infraestruturas tecnológicas, como *softwares* utilizados (seus licenciamentos e atualizações), antivírus entre outros; ii) revisão do armazenamento e segurança de dados analógicos, bem como o acesso aos arquivos físicos; iii) revisão dos dados já coletados e em uso pela instituição, assim como dos contratos vigentes para que contemplem cláusulas referentes à proteção de dados pessoais; iv) elaboração ou revisão das políticas internas de proteção de dados e de segurança da informação; v) criação de mecanismos, como um portal da privacidade, por onde o titular possa exercer os seus direitos de informação, acesso, retificação, oposição, entre outros; e vi) elaboração de um sistema de gestão de crise para que possa se posicionar com sabedoria em caso de incidente de segurança da informação (ABRUSIO, *et al*, 2020).

Portanto, o descumprimento dos mecanismos abrangidos nesse pilar poderá causar impactos econômicos, reputacionais, legais, regulatórios, de mercado e/ou operacionais.

Logo, é importante que ocorra análise periódica de riscos e atualização das políticas criadas para mitigar riscos e identificar situações de risco.

2.4. ESTRUTURAÇÃO DAS REGRAS E INSTRUMENTOS

Com base no conhecimento do perfil e riscos da instituição, deve-se elaborar ou atualizar as diretrizes internas de *compliance* como o código de conduta e políticas aplicáveis, principalmente às áreas que possuam algum contato com manejo de dados pessoais.

Para uma cultura interna ainda mais focada em proteção de dados, é possível estabelecer parâmetros dos valores da instituição até mesmo dentro de seu Código de Conduta, estabelecendo vedações expressas a atos que possam ocasionar violações à LGPD. Os padrões de conduta devem ser claros e objetivos para possibilitar um amplo entendimento em todos os níveis hierárquicos dentro da empresa.

É imprescindível a implementação e desenvolvimento de procedimentos de prevenção e detecção de irregularidades. Após a estruturação do Programa de *Compliance* em proteção de dados pessoais, e da instância interna responsável, a instituição deve comunicar e treinar os colaboradores nas novas (ou atualizadas) regras.

No que tange a detecção de indícios da ocorrência de violações à LGPD e ao Programa de *Compliance* em relação aos dados, é recomendável uma investigação interna, que servirá como base para que sejam tomadas as providências cabíveis. Além disso, as normas internas devem tratar de aspectos procedimentais a serem adotados nas investigações como: (i) prazos; (ii) responsáveis pela apuração das denúncias; e (iii) identificação da instância ou da autoridade para a qual os resultados das investigações deverão ser reportados.

2.5. ESTRATÉGIAS DE MONITORAMENTO

Para evitar a sujeição da instituição em eventual incidente de violação à LGPD, é fundamental que procedimentos de verificação da aplicabilidade do Programa de *Compliance* de dados pessoais estejam adequados ao modo de operação da instituição, além da criação de mecanismos para que as deficiências encontradas em qualquer área possam realimentar continuamente seu aperfeiçoamento e atualização. É preciso garantir, também, que o Programa de *Compliance* em proteção de dados pessoais seja parte da rotina da instituição e que atue de maneira integrada com outras áreas correlacionadas, alcançando a aderência de todos.

O monitoramento pode ser feito mediante a coleta e análise de informações de diversas fontes, tais como: (i) relatórios regulares sobre as rotinas do Programa de *Compliance* de dados ou sobre investigações relacionadas; (ii) tendências verificadas nas reclamações dos clientes da empresa; (iii) informações obtidas do canal de denúncias; e (iv) relatórios de agências governamentais reguladoras ou fiscalizadoras. Ademais, o Programa de *Compliance* de dados, deve ser entendido como uma estrutura orgânica, que somente funcionará caso exista harmonia e conexão entre seus pilares, como o monitoramento contínuo, por exemplo, pode indicar a necessidade de revisão de algumas regras e instrumentos; o mesmo ocorrendo no caso de mudança no cenário de riscos da empresa.

O comprometimento da alta administração e a autonomia da instância responsável pelo Programa, por outro lado, são fatores determinantes para a implementação das regras e instrumentos estabelecidos, em especial daqueles relacionados à aplicação de penalidades e remediação de irregularidades.

3. CONSEQUÊNCIAS LEGAIS DE UM PROGRAMA DE *COMPLIANCE* INADEQUADO À LGPD

Conforme tratado na seção anterior, o Programa de *Compliance* é de caráter preventivo, ou seja, estabelece uma série de diretrizes de boas práticas a fim de evitar eventuais violações. E no âmbito da LGPD, as empresas que instituem medidas adequadas, não estão imunes ao descumprimento destas. Ou seja, em caso de violação ou vazamento de dados, demonstram por si próprias a possibilidade de que mesmo após implementadas todas as medidas necessárias, para inibir um incidente de segurança com dados pessoais, haverá um possível risco de ocorrer um descumprimento da LGPD.

A exemplo, pode-se mencionar a recente ação movida pelo Sindicato dos Trabalhadores nas Indústrias de Alimentação de Montenegro em face da JBS, alegando que haveria descumprimento sistemático da proteção de dados. Em síntese, ocorreu supostamente o compartilhamento de dados pela JBS para outros controladores e operadores sem as cautelas necessárias, sem indicar o encarregado pelos dados pessoais e por intermédio da internet, desrespeitando a intimidade, a privacidade e a imagem. E neste caso, a juíza Ivanise Marilene Uhlig de Barros observou que a empresa possui um manual de privacidade, que designa um encarregado e mostra as adequações da estrutura empresarial à Lei Geral de Proteção de Dados (LGPD). "Também o portal de transparência indicado à defesa e as cartilhas de informação apresentadas revelam atendimento aos critérios principiológicos de livre acesso e transparência", acrescentou (HIGÍDIO, 2021, p. 2). No caso

em tela, pode-se observar que a empresa se valeu de mecanismos internos para demonstrar sua adequação e obteve êxito ao comprovar as medidas adotadas dentro de sua estrutura empresarial.

Nesse sentido, autores aplicados no estudo do *compliance* de dados pessoais asseveram (FRAZÃO; OLIVA; ABILIO, 2019, p. 711):

> a implementação de mecanismos de *compliance* também configura elemento de demonstração do tratamento regular dos dados pessoais pelo agente de tratamento – especialmente relevante para buscar (i) afastar sua responsabilidade com base no art. 43, inciso II; e/ou (ii) comprovar o cumprimento de determinados deveres cujo ônus da prova pode lhe ser imposto (arts. 8º, § 2º; e 42, § 2º) [...]

Portanto, prova-se que investir em um Programa de *Compliance*, pode favorecer a empresa em muitos aspectos e principalmente econômico.

Se por um lado, há essa vantagem para aquelas empresas que estão em atendimento às normas de proteção de dados, por outro, temos as consequências legais para aquelas que não trataram de instituir um Programa de *Compliance* em proteção de dados pessoais adequado, e que como desdobramento pela não adoção de mecanismo preventivo, se põem suscetíveis e expostas às sanções administrativas decorrentes de violações.

3.1. SANÇÕES ADMINISTRATIVAS

A LGPD determina que a partir de agosto de 2021, poderão incidir as multas aplicadas pela Autoridade Nacional de Proteção de Dados, órgão federal criado para regular e fiscalizar a aplicação da LGPD.

O artigo 52 da LGPD estabelece que, caso ocorra violação às normas nela previstas, a Autoridade Nacional poderá aplicar as sanções de: (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 (BRASIL, 2018).

Nota-se uma linha crescente de gravidade que poderá impactar a empresa responsável pela infração de diversas formas, e para além do impacto econômico, a imagem da empresa pode ser fortemente prejudicada com publicização da infração e consequentemente, no caso de uma companhia aberta, por exemplo, poderá influenciar diretamente no valor das ações com a redução de seu valor de mercado.

Além disso, se a empresa não estiver preparada para responder prontamente a um incidente de vazamentos, por exemplo, poderá haver uma suspensão de exercício de atividade, a depender do porte da empresa e, além disso, poderia ocasionar na inviabilização da empresa.

Outrossim, as empresas que se encontram em processo de adequação/instituição de um Programa de *Compliance* em dados pessoais e tomaram as medidas preventivas e estão prezando pela sua manutenção antes mesmo da vigência da LGPD, se colocam em vantagem, menos suscetíveis a violações à LGPD e incorrerem em sanções advindas desta.

CONSIDERAÇÕES FINAIS

Vivemos uma era em que os dados se tornaram demasiados valiosos e mais do que nunca, a colocação de que “os dados são o novo petróleo” (Humby, 2006) ganha ainda mais força, exigindo uma transparência inerente a quem lida com esse insumo tão precioso e o advento da LGPD enaltece a conformidade e o tratamento consciente dos dados pessoais.

A iniciativa privada brasileira se deparou com mais um desafio de adequação à LGPD e instituição de boas práticas deliberadamente e intencionalmente voltadas à proteção de dados pessoais. Evidentemente, que o cenário ainda está em construção e recorrentemente são feitas projeções para o futuro, mas a constante é: não há como retroceder.

O Programa de *Compliance* enquanto mecanismo de efetivação e adoção à LGPD é um meio para que sejam cumpridas as diretrizes que necessitam ser demandas do mais alto escalão de uma empresa. Se faz necessário enxergar essa ferramenta não como um custo adicional à empresa, mas como um investimento de caráter preventivo que servirá de apoio e guia para estar efetivamente em conformidade à LGPD. Vimos, que isso requer um comprometimento de diversas instâncias de uma empresa para que se esteja em constante observância, além da análise comparativa dos pilares de integridade.

Ademais, em caso de desatendimento às normas estabelecidas pela LGPD e eventuais infrações, há uma demanda que pode ser onerosa para uma reparação prontamente eficaz, e, portanto, a figura do Programa de *Compliance* em proteção de dados pessoais se torna ainda mais fundamental.

REFERÊNCIAS

ABRUSIO, Juliana *et al*. OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS EM INSTITUIÇÕES DE ENSINO. OPICE BLUM ACADEMY, [s. l.], p. 1-13, 2020. Disponível em: https://opiceblumacademy.com.br/wp-content/uploads/2021/05/Cartilha-Os-impactos-da-LGPD-nas-instituicoes-de-ensino.pdf. Acesso em: 15 dez. 2020.

ARTHUR, Charles. *Tech giants may be huge, but nothing matches big data.* ***The Guardian****,* 23 ago. de 2013. Disponível em: https://www.theguardian.com/technology/2013/aug/23/tech-giants-data. Acesso em: 29 de jul. 2021.

BANDEIRA, Ingrid Santos et al. Impactos da Lei Geral de Proteção de Dados Pessoais no Programa de Compliance. In: FRANCO, Isabel. **Guia Prático de Compliance**. 1. ed. Rio de Janeiro: Forense, 2020. cap. 22, p. 443 - 454.

BARCAT, George. **Governança Corporativa e Integridade Empresarial:** dilemas e desafios. 1. ed. São Paulo: SaintPaul. 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 15 de fev. de 2021.

CUEVA, Ricardo Villas Bôas. Funções e finalidades dos programas de compliance. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana. **Compliance**: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Ed. Renovar, 2006.

FRAZÃO, Ana. Dever de diligência: Novas perspectivas em face de programas de compliance e de atingimento de metas. **Jota**, [*S. l.*], 15 fev. 2017. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/dever-de-diligencia-15022017. Acesso em: 22 mar. 2021.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 99-29 e p. 677-715.

G1, Globo. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**, 20 mar. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml> Acesso em: 15 fev. 2021.

HIGÍDIO, José. Justiça rejeita ação de sindicato que acusava JBS de violações à LGPD. **Consultor Jurídico**, [*S. l.*], p. 1-3, 14 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-14/justica-rejeita-acao-sindicato-acusava-jbs-violacoes-lgpd. Acesso em: 17 jul. 2021.

JIMENE, Camilla do Vale. Das Boas Práticas e da Governança. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD:** Lei Geral de Proteção de Dados Pessoais comentada. 3. ed. São Paulo: Thomson Reuters Brasil, 2021. cap. CAPÍTULO VII, SEÇÃO II, p. RL-1.14 - RL-1.15. Disponível em: https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fcodigos%2F188730949%2Fv3.4&titleStage=F&titleAcct=i0ad62b780000017a2ed87d389d2af0ad#sl=0&eid=3b3c168443d706d6d4f8a8cd02dd603c&eat=%5Bereid%3D%223b3c168443d706d6d4f8a8cd02dd603c%22%5D&pg=1&psl=p&nvgS=false. Acesso em: 16 jun. 2021.

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, p. 50 – 69. 2020.

MENEZES, Joyceane Bezerra de; COLAÇO, Hian Silva. Quando a lei geral de proteção de dados não se aplica. *In:* TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 161.

Ministério da Justiça, Conselho Administrativo de Defesa Econômica [“Cade”]. **Guia Programas de Compliance.** Distrito Federal, 2016. Disponível em: http://antigo.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-versao-oficial.pdf. Acesso em 26/03/2021.

MORAES, Henrique Fabretti. Sistemas de Compliance, Programas de Privacidade e DPO, *In* **Data Protection Officer [Engarregado]:** Teoria e Prática de Acordo com a LGPD e o GDPR. São Paulo: Ed. Revista dos Tribunais, 2020. p. 546-547.

OLIVEIRA, Samuel Rodrigues de; ABRUSIO, Juliana; RONCAGLIA, Ana Maria. A importância da análise e gestão de riscos no tratamento de dados pessoais. **Consultor Jurídico**, [*S. l.*], p. 1-6, 13 jul. 2021. Disponível em: https://www.conjur.com.br/2021-jul-13/direito-digital-importancia-analise-gestao-riscos-tratamento-dados-pessoais. Acesso em: 15 jul. 2021.

PANCINI, Laura. Amazon recebe multa recorde de US$ 887 milhões da União Europeia. **EXAME**. 30 jul. 2021. Disponível em: <https://exame.com/tecnologia/amazon-multa-recorde-da-uniao-europeia/> Acesso em: 02 set. 2021.

SIMÃO, Valdir Moysés *et al*. Programa de Integridade: Diretrizes para Empresas Privadas. **Controladoria Geral da União, Brasília** - DF, p. 1-28, 2015. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas-privadas.pdf. Acesso em: 19 nov. 2020

UNITED STATES OF AMERICA. **United States Setencing Comission**. Disponível em: https://www.ussc.gov/guidelines/2018-guidelines-manual-annotated. Acesso em: 14 dez. 2020.

Contatos: julysamarys@gmail.com e marco.florencio@mackenzie.br