A LEI GERAL DE PROTEÇÃO DE DADOS E COMPLIANCE NA ERA DIGITAL SOB A ESFERA DAS ORGANIZAÇÕES EMPRESARIAIS

Caroline Ruback (IC) e Marco Antônio Loschiavo Leme de Barros (Orientador)
Apoio: PIBIC Mackpesquisa

RESUMO: O presente artigo tem como principal objetivo a análise da aplicabilidade da Lei Geral de Proteção de Dados (LGPD) em conjunto com o Compliance nas organizações empresariais, a partir de seus fundamentos e de suas consequências na prática por meio do método científico de caráter dedutivo, tendo como base pesquisas bibliográficas e sustentadas por referenciais teóricos de caráter exploratório, como doutrinas especializadas, artigos, trabalhos monográficos, além de pesquisas documentais, artigos de lei, decisões judiciais e outros atos normativos. Diante disso, evidenciar a importância das adequações normativas, as quais as empresas estão sujeitas a sofrer possíveis penalizações administrativas, conforme diretrizes da LGPD. Considerando que todas as organizações empresariais precisam estar em conformidade com a nova regulamentação, este estudo tem como viés expor as diretrizes e a importância das boas práticas de governança do Compliance para a proteção aos dados pessoais com a regulamentação da LGPD no âmbito empresarial. No entanto, com a análise sobre a importância do direito à privacidade aos dados pessoais em tempos de uma era digital. A pesquisa concluiu que é evidente a conexão entre os princípios da LGPD e os conceitos da governança corporativa, que buscam incorporar as normas estatais nos procedimentos internos das organizações empresariais.

Palavras-chave: Lei Geral de Proteção de Dados. Compliance. Organizações Empresariais.

ABSTRACT: The main objective of this article is to analyze the applicability of the General Data Protection Law (LGPD) in conjunction with Compliance in business organizations, based on its foundations and its consequences in practice through the scientific method of a deductive nature, based on bibliographic research and supported by theoretical references of an exploratory nature, such as specialized doctrines, articles, monographic works,

in addition to documentary research; articles of law, judicial decisions and other normative acts. In view of this, highlight the importance of regulatory adjustments, since companies are subject to possible administrative penalties, according to the LGPD guidelines. Considering that all business organizations need to be in compliance with the new regulation, this study aims to expose the guidelines and the importance of good Compliance governance practices for the protection of personal data with the LGPD regulation in the business scope. However, with the analysis of the importance of the right to privacy of personal data in times of a digital age. The research concluded that the connection between the LGPD principles and the concept of corporate governance is evident, which seeks to incorporate state norms into the internal procedures of business organizations.

Keywords: General Data Protection Law. Compliance. Business Organizations.

I. INTRODUÇÃO

Ao pensarmos na Era Digital, logo associamos uma sociedade movida a dados, que constantemente vem sendo marcada pela crescente dependência da sociedade em relação a tecnologia. Diante disso, a tecnologia oferece muitas oportunidades e benefícios para as empresas e a sociedade como um todo. Mas é fundamental garantir que esses avanços tecnológicos sejam acompanhados de proteção e integridade aos usuários.

A Era Digital ocasionou uma série de mudanças significativas para o mundo empresarial, incluindo o aumento da conectividade, o avanço tecnológico de ferramentais de negócios capazes de processar e transmitir informações em uma quantidade de velocidade imaginável. Com isso, os desafios empresariais de preservação às boas práticas aumentam.

A revista *The Economist* de 06.05.2017[1i], estampou em sua capa a manchete "*The world's most valuable resource",* a evidenciar os dados como uma nova mercadoria para o mundo, os dados atualmente são vistos como uma indústria lucrativa de rápido crescimento, logo, os dados se tornaram primordial para a sociedade. Mas quanto maior a coleta de dados, maior será a vulnerabilidade da sociedade.

Com a inserção dos dados pessoais na sociedade seja com o consentimento do usuário ou apenas com seu uso contínuo em redes sociais, cada usuário que opta por compartilhar conteúdos em sua rede social por razões pessoais se submetem ao *"opt-in"* que logo significa que o usuário opta de forma deliberada e expressa o seu consentimento em compartilhar seus próprios conteúdos. Dessa forma, empresas conseguem coordenar com a análise dos dados pessoais um perfil de cada usuário, delimitando um *overview* com suas preferências e interesses para apresentá-las diferentes tipos de publicidades e postagens.

Contudo, muitas vezes, estes dados são monetizados por empresas, que lucram com a venda ou com troca de informações, com a intenção de se anteciparem com os pensamentos futuros dos usuários. — "uma nova ordem

[1] Disponível em: [www.economist.com/leaders/2017/]. Acesso em 17.05.23.

econômica que reivindica a experiência humana como matéria-prima para práticas comerciais dissimuladas de extração, previsão e vendas"[2].

O escândalo envolvendo a empresa Cambridge Analytica evidência a monetização de dados pessoais entre as empresas, a qual é 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 conseguiu realizar um verdadeiro estudo comportamental de seus usuários, chegando a prever suas possíveis ações e tomadas de decisões, acarretando a interferência das eleições de 2016 dos EUA e no Brexit.[3]

A evidência da monetização dos dados pessoais consiste apenas em uma das inúmeras vulnerabilidades que os usuários estão sujeitos nesta Era Digital. Desse modo, a importância com a segurança dos dados pessoais dos usuários na sociedade se torna de extrema urgência com a necessidade de adotar mecanismos eficazes para evitar possíveis vazamentos e garantir a segurança dos dados. Contudo não se limitando apenas na privacidade dos dados pessoais dos usuários, mas sobre a ingerência de organizações empresariais.

A problemática advinda da insegurança do compartilhamento de dados pessoais é apontada no mundo jurídico há tempos, antes mesmo da expansão do mundo digital devido a várias razões fundamentais. Mas uma delas é com a privacidade e os direitos individuais dos indivíduos na sociedade, logo, por ser um direito garantido como fundamental para a jurisdição. Conforme, o trecho de voto do Ministro Ruy Rosado de Aguiar de 1995 que já constatava a preocupação com a manipulação de dados pessoais:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos

---

[2] ZUBOFF, Shoshana. A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2021, p. 13.

[3] Disponível em: [The Guardian, https://www.theguardian.com/news/series/cambridge-analytica-files] Acesso em 27.07.23.

> pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. (BRASIL, STJ, 1995).[4]

A preocupação exposta pelo Ministro Ruy Rosado de Aguiar se robustece na Era Digital em que vivemos, de modo a comprovar que quanto mais expostos os dados pessoais dos usuários, mais vulneráveis e menos independentes de suas escolhas podem ficar. A título de exemplo, em 2018, o Banco Inter, um dos pioneiros em oferecer contas digitais no país, registrou um vazamento que deixou vulnerável cerca de 19 mil correntistas. O vazamento dos dados aconteceu em uma ação que envolveu o envio, por um suposto hacker, de um arquivo criptografado que teria como conteúdo senhas, códigos de verificação, cheques, declarações de imposto de renda e dados pessoais dos clientes do banco. Em dezembro do mesmo ano, a empresa fechou um acordo com o Ministério Público e pagou uma multa de R$ 1 milhão, que foi destinada a instituições públicas de caridade e a organizações que trabalham combatendo o crime cibernético[5]. Por consequência, o ordenamento jurídico se aprimora para melhor adequar o direito à privacidade e garantir seus direitos e garantias fundamentais a sociedade.

Entretanto, após os escândalos em ordem internacional da empresa Cambridge Analytica a preocupação com os dados pessoais aumentou e foi de um escândalo histórico à decisão para a conclusão da discussão e criação do

[4] Disponível em: [https://scon.stj.jus.br/SCON/]. Acesso em: 10.07.23.

[5] Disponível em: [https://tecnoblog.net/noticias/2018/12/19/banco-inter-acordo-mpdft/]. Acesso em: 18.08.23.

General Data Protection Regulation (GDPR)[6]. A lei criada pela União Europeia com objetivo de defender a privacidade dos usuários.

No Brasil o início de debates sobre uma lei geral de proteção de dados começou através da submissão do primeiro anteprojeto de lei do Poder Executivo em dezembro de 2010, que teve como principal inspiração a norma da União Europeia que trata de proteção de dados, a Diretiva 95/46/EC.

O anteprojeto contou com 794 contribuições durante o perídio de 5 meses de consulta pública, que se baseava em um rol de princípios de proteção de dados pessoais extraídos das melhores práticas da regulação internacional: finalidade, necessidade, proporcionalidade, qualidade, transparência, segurança e livre acesso.[7]

Com a aprovação do Congresso Nacional, o Projeto de Lei foi encaminhado ao Presidente da República para sanção. Em agosto de 2018, a Lei Geral de Proteção de Dados foi sancionada, estabelecendo um período de transição para a sua efetiva entrada, entrando em vigor em 18 de setembro de 2020, entretanto, estabelecendo um período de adaptação para as empresas e órgãos governamentais se adequassem às suas disposições.

Diante disso, a proteção de dados pessoais se tornou uma preocupação crescente em todo o mundo. Com isso, a Lei Geral de Proteção de Dados estabelece regras claras para a coleta, armazenamento, processamento e compartilhamento, com o principal objetivo de proteger e resguardar os dados pessoais.

À medida em que as empresas armazenam e compartilham os dados, elas precisam garantir que esses dados estejam protegidos conforme determina a Lei Geral de Proteção de Dados. Todavia, as empresas organizacionais enfrentam desafios e riscos, visto que, a coleta e o uso inadequado de dados podem levar à violação da privacidade e dos direitos

---

[6] “Ainda faltava o ingrediente mais quente para eclodir a pauta da proteção de dados pessoais em 2018: o escândalo da Cambridge Analytica escancarou como a desproteção de dados pessoais impacta não só a vida de um cidadão em específico, mas de toda uma coletividade e os alicerces do que se entende por democracia. Logo depois, houve uma sessão temática no Senado para debater, pela primeira vez no plenário em uma das Casas do Congresso Nacional, o tema. E, em maio de 2018, a Câmara dos Deputados realizou também um seminário como decorrência do referido escândalo”. (BIONI, 2018, p.1).

[7] Disponível em: [https://www.aasp.org.br/revista-do-advogado/] Acesso em 27.07.23.

individuais dos usuários. Além disso, a utilização de dados pode gerar em desigualdades e discriminação quando usados para tomada de decisões automáticas em redes sociais, conforme exposto acima.

Nesse sentido, as empresas organizacionais se deparam com um enorme desafio para se adequarem a uma nova legislação e de estabelecerem novas normas governamentais em seu ambiente corporativo. Contudo, a LGPD incentiva a adoção de boas práticas e governança ao dispor em seu artigo 50, § 2º, objetivos mínimos a serem atendidos pelas organizações empresariais. Com isso, estabelece a importância dos programas de Compliance, para uma criação educativa corporativa de respeito à ética e às regras da empresa.

II. A LEI GERAL DE PROTEÇÃO DE DADOS E SEUS PRINCÍPIOS

A Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018 tem como objetivo estabelecer regras claras e objetivas para o tratamento de dados pessoais no Brasil. A lei se aplica à todas as empresas que coletam, armazenam, compartilham ou utilizam dados pessoais, incluindo aquelas que atuam no ambiente digital.

Legalmente inspirada na Lei de Proteção de Dados da União Europeia, o General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados instituiu seus fundamentos baseando-se nos direitos fundamentais de liberdade e privacidade, na proteção da dignidade humana, na livre iniciativa, na livre concorrência e no desenvolvimento econômico e tecnológico.

Segundo Patrícia Peck[8], “a LGPD e o GPDR, ambas as legislações têm como objetivo o regramento do tratamento de dados pessoais buscando em si a defesa dos direitos fundamentais das pessoas naturais”. Essas legislações definem o que são dados pessoais, estabelecendo o consentimento como um dos fundamentos centrais nas relações que envolvam dados pessoais, com previsão de aplicações de medidas de segurança e sanções no caso de descumprimento, prevendo um órgão competente para fiscalizar e zelar pela proteção dos dados pessoais e da privacidade.

---

[8] PINHEIRO, 2018, p.38. Proteção de dados pessoais. Comentários Lei 13.709/2018 (LGPD).

Pode-se pontuar que a necessidade de leis especificas para a proteção de dados pessoais aumentou com o rápido desenvolvimento e a expansão da tecnologia no mundo, como resultado dos desdobramentos da globalização, que trouxe como uma de suas consequências o aumento da importância da informação. Isso quer dizer que a informação passou a ser um ativo de alta relevância para governantes e empresários: quem tem acesso aos dados, tem acesso ao poder[9].

Considerada como o eixo normativo que compatibiliza a máxima de tutela do indivíduo no seu núcleo essencial de privacidade, com base na conformidade com regulamentações e leis que protegem os dados dos consumidores, a Lei Geral de Proteção de Dados, também é considerada um desafio. As empresas precisam garantir que estão em conformidade com as leis aplicáveis e adotar medidas para proteger os dados pessoais de seus clientes.

Diante disso, a LGPD busca garantir a proteção da privacidade e dos dados pessoais dos indivíduos, incentivando a inovação e o desenvolvimento econômico de forma ética e responsável. Com isso, aborda em seu artigo 6º[10]

---

[9] PINHEIRO, 2018, p. 50. Proteção de dados pessoais. Comentários Lei 13.709/2018 (LGPD).

[10] Artigo 6º: As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - Finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - Livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - Qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - Transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - Segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - Responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

os princípios estabelecidos que devem ser seguidos pelas organizações ao realizarem tratamento de dados pessoais.

A base principiológica estabelecida pela Lei Geral de Proteção de Dados desempenha um papel fundamental na erradicação de questões problemáticas em diversos ramos do direito. Ao fornecer um conjunto de princípios claros e orientadores, a LGPD não apenas protege a privacidade dos cidadãos, mas também estabelece um padrão ético e legal que pode ser adaptado para abordar desafios em áreas variadas. Através de princípios como finalidade, necessidade, consentimento, transparência, segurança e responsabilização, a legislação não apenas regula a coleta e o processamento de dados pessoais, mas também estabelece uma base sólida para garantir práticas legítimas e éticas em transações comerciais, relações de consumo, pesquisas científicas, processos judiciais e governança pública. Dessa forma, a LGPD transcende sua aplicação estrita no âmbito da privacidade digital, emergindo como um instrumento poderoso para a promoção da justiça, da equidade e do respeito aos direitos individuais em toda a gama dos ramos do direito.

Os princípios finalidade, adequação e necessidade são responsáveis por direcionar o tratamento dos dados pessoais, respeitando a correlação entre o tratamento dos dados e a finalidade do uso[11]. Para trazer maior segurança e transparência ao processo. O livre acesso está expresso no caput do artigo 9º, mas está implícito nos artigos. 18, 19 e 20. Todos esses dispositivos tratam de formas de requisição e acesso do titular às informações que lhe digam respeito, assim como as prerrogativas de solicitar a correção de equívocos ou revisão

[11] "Um princípio fundamental que todas as atividades de processamento de dados devem seguir é o princípio da finalidade, que indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Esse princípio é essencial para se limitar o acesso de terceiros ao banco de dados. De forma semelhante, ele também serve como parâmetro para julgar se determinado uso dos dados pessoais é adequado e razoável, de acordo com a finalidade informada no primeiro momento ao interessado. (Doneda, 2006, p.216). Por fim, esse princípio exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas (Rossangel, 2003, p.140)". MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. Revista de Direito do Consumidor, v.20, n.79, jul./set. 2011, p. 45/81.

de decisões subsidiadas em procedimentos exclusivamente automatizados sobre seus dados[12].

O princípio da qualidade dos dados exige que os dados sejam objetivos, exatos e atualizados. Esse princípio se relaciona, em grande medida, com os princípios da transparência e do livre acesso, na medida em que esses asseguram o conhecimento e os meios de correção de informações equivocadas[13]. Considera-se, porém, que a essência desse princípio está no inciso III do artigo 18.

O princípio da transparência é considerado um dos mais presentes ao longo de toda legislação. Ele transparece no artigo 9º; artigo 10, §2º; no artigo 18, I, II, VII e VIII; e no artigo 20. Mas enfatizando o artigo 9º que se prende à questão da transparência das informações do tratamento de dados, apontando quais as características relativas ao acesso à informação. Nesse sentido, a clara exposição e o fácil acesso relativo à finalidade do tratamento, assim como sua forma, duração, além das informações acerca dos agentes que realizam o tratamento, são elementos essenciais. A gratuidade de consultar a essas informações também é uma garantia importante.[14]

Os princípios da segurança, da presença e da responsabilidade, ou prestação de contas, também são bastantes próximos. Isso, porque o primeiro visa a evitar situações ilícitas, ao passo que o segundo pretende evitar o dano à pessoa por causa do tratamento inadequado dos dados pessoais. Não obstante, o ilícito e o dano são conceitos clássicos da responsabilidade civil.[15]

A prevenção é um princípio que complementa ao princípio da segurança, impondo que os agentes de tratamento adotem as medidas necessárias para prevenir que danos ocorram em razão do tratamento de

---

[12] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVIA. Milena Donato. Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. Revista dos Tribunais, 2º Ed. São Paulo, p. 74, 2020.

[13] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVIA. Milena Donato. Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. Revista dos Tribunais, 2º Ed. São Paulo, p. 75, 2020.

[14] PINHEIRO, 2018, p. 110. Proteção de dados pessoais. Comentários Lei 13.709/2018 (LGPD).

[15] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVIA. Milena Donato. Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. Revista dos Tribunais, 2º Ed. São Paulo, p. 76, 2020.

dados pessoais. É mais amplo que a segurança porque deveria ser interpretado como atividades não necessariamente técnicas, mas de governança e preparo para gestão de crises.[16]

A não discriminação é um princípio que há tempos já tinha conquistado espaço nas legislações internacionais, com a identificação e o tratamento diferenciado da categoria dos dados sensíveis. Esses são identificados como os dados que contêm informações que podem levar à discriminação da pessoa, como origem étnica, religião, orientação sexual e posição política.[17]

Para completar o rol dos princípios que balizam a Lei Geral da Proteção de Dados, o Princípio da Responsabilização e Prestação de Contas, que obriga o controlador dos dados pessoais à realização de condutas e de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. O objetivo é assegurar o titular dos dados um amplo controle daquilo que está sendo feito com seus dados.

Os princípios indicados na LGPD refletem a formação de um sistema de proteção de dados, pois nenhum deles representa uma novidade em si, mas a cristalização de avanços que foram alcançados pelas leis anteriores, muitas vezes com viés mais pragmático do que principiológico.[18]

Conforme exposto, é fundamental que todos os princípios sejam seguidos conforme determinado em lei, e que todos os titulares estejam cientes da utilidade de seus dados. Entretanto, para esse propósito a LGPD dedica-se

---

[16] GUILHERME, Luiz Fernando do Vale de Almeida. Manual de Proteção de Dados: LGPD comentada. São Paulo: Almedina, 2021.

[17] "Quando se fala em proteção de dados pessoais deve ser trazida à baila a questão dos dados sensíveis, que são aqueles caracteres pessoais que revelam a origem racial, ao opiniões políticas, as convicções religiosas ou outras, bem como os relativos à saúde, à vida sexual, às condições penais, etc. [...] A distinção dessa categoria de dados, segundo Doneda, é o fruto de uma observação pragmática de diferença que a divulgação deste tipo de informação merece em relação as demais, pois revelam a presença de outros valores dignos de tutela além da privacidade, como a igualdade material. A diferença é realizada tendo em vista que determinados dados possibilitariam uma utilização ainda mais discreta da informação pessoal, sendo devida a sua proteção não só em consagração ao direito à privacidade, mas também para proteger a dignidade da pessoa humana e os direitos à liberdade e à igualdade". SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. Revista de Direito Civil Contemporâneo, v. 9, ano 3, out-dez. 2016, p. 49-104.

[18] FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVIA. Milena Donato. Lei Geral de Proteção de Dados e suas repercussões no direito brasileiro. Revista dos Tribunais, 2º Ed. São Paulo, p. 81, 2020.

a Seção II do Capítulo VII ao tratamento das boas práticas e da governança, buscando auxiliar as empresas organizacionais com a adequação de um bom programa de Compliance de Dados.

Em 2021, 145 países dispunham de leis sobre a privacidade e proteção de dados pessoais, evidenciando uma preocupação global quanto à regulamentação do tema (Greenleaf, 2021). A aprovação de leis que impõem um crescente controle ao tratamento de dados pessoais vem colocando desafios às empresas de todo o mundo, na medida em que rotinas estabelecidas devem ser alteradas e o fortalecimento de uma cultura de proteção de dados precisa ser fomentada, ao mesmo tempo que investimentos devem ser direcionados à melhoria da segurança digital.[19]

Desse modo, relação entre a base principiológica da LGPD e o compliance é de fundamental importância para as organizações que buscam operar de forma ética e legal no tratamento de dados pessoais. Os princípios estabelecidos na LGPD, como finalidade, necessidade, transparência e responsabilização, não apenas delineiam as diretrizes para a coleta e o processamento de dados, mas também servem como alicerces sólidos para a construção de programas de compliance eficazes. Ao aderir e implementar esses princípios, as organizações não apenas garantem a conformidade com a legislação de proteção de dados, mas também cultivam uma cultura corporativa de respeito à privacidade e à segurança das informações pessoais.

O compliance com a LGPD envolve a adoção de políticas e práticas que reflitam os valores embutidos nos princípios da lei, assegurando que os processos de tratamento de dados estejam alinhados com os mais altos padrões éticos e legais. Ou seja, a base principiológica da LGPD é um guia essencial para as iniciativas de compliance, permitindo que as organizações construam relações de confiança com seus clientes, parceiros e stakeholders, ao mesmo tempo em que mitigam riscos jurídicos e reputacionais.

---

[19] “Dificuldades semelhantes foram relatadas para que as empresas europeias buscassem se adequar ao Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation [GDPR]). Em um momento inicial, diversas empresas fizeram o uso de medidas paliativas para adequação, sendo que muitos desafios ainda são persistentes, tais como relatórios de impacto e auditorias, que são pouco presentes”. (Mikkelsen et al., 2019)

III. COMPLIANCE: ASPECTOS E CONCEITO

As empresas precisam estar em conformidade com as leis e regulamentações, além de garantir a ética e a segurança na aplicabilidade de suas políticas internas. Com isso, a necessidade de as empresas estarem em conformidade com as leis e regulamentações vai muito além de uma mera obrigação legal; é um imperativo ético e uma estratégia inteligente para construir uma base sólida de confiança e credibilidade. As empresas, ao lidarem com informações confidenciais e pessoais, assumem uma posição de confiança em relação aos usuários cujos dados são processados. Isso inclui a implementação de políticas claras de proteção de dados, treinamentos para os funcionários, monitoramento e revisão contínuas e canais de denúncia para a identificação de possíveis irregularidades dentro das organizações empresariais.

Com isso, o programa de Compliance deve ser implementado em todas as áreas da empresa que lidam com dados pessoais por diversas razões essenciais. Primeiramente, os dados pessoais são um ativo valioso e sensível, e sua coleta, processamento e armazenamento devem ser conduzidos de maneira consistente e regulamentada para garantir a proteção dos direitos dos indivíduos. Ao aplicar o programa de Compliance em todas as áreas, a empresa assegura uma abordagem uniforme e coerente em relação à privacidade dos dados, evitando discrepâncias ou práticas inadequadas que poderiam levar a violações ou vazamentos de informações. Além disso, a empresa deve adotar uma abordagem proativa de gestão de riscos relacionados à privacidade, incluindo a realização de análises de impacto à privacidade e a implementação de planos de contingência em caso de incidentes.

Ademais, a adoção de um programa de compliance adequado que envolve a implementação de um conjunto abrangente de medidas, práticas e políticas que garantam que uma organização esteja operando em conformidade com as leis, regulamentações, normas e padrões relevantes é fundamental para as empresas que buscam cumprir as obrigações legais e promover a confiança dos clientes e usuários, logo gerando benéficos para o meio empresarial. Além disso, um programa de compliance bem-sucedido não se limita apenas ao cumprimento de requisitos legais, mas também promove uma cultura ética e responsável dentro da organização. Assim como as empresas que adotam boas práticas de conformidade e adequação podem

obter uma vantagem competitiva no mercado, uma vez que a conformidade com as leis é cada vez mais valorizada pelos clientes e usuários.

O termo Compliance, que tem como origem a expressão inglesa “to comply”, com a tradução significativa de conformidade, representa que as empresas estejam em conformidade com normas e regulamentos vigentes, que faz com que a Lei Geral de Proteção de Dados se torne um pilar justamente com o Compliance entre as organizações empresariais. Assim sendo, é de extrema importância para a implementação de conformidade nas empresas, pois se trata de uma legislação que impõe obrigações e responsabilidades significativas às organizações em relação à coleta de dados pessoais.

No Brasil, o termo Compliance surgiu a partir da Lei 12.846/2013, como “Lei Anticorrupção”, que determina a responsabilização das organizações pela prática de atos lesivos à administração pública. Isto posto a preocupação das organizações empresariais quanto a possibilidades de arcar com sanções em prol de processos administrativos de responsabilização, se tornando um instrumento fundamental de controle de processos e sustentabilidade empresariais.

Nesse contexto, o Compliance atua como um conjunto de medidas e práticas que as empresas devem implementar para garantir que suas operações estejam em conformidade com a LGPD. O objetivo é assegurar que as organizações que realizam o tratamento de dados pessoais revejam as suas práticas para torná-las adequadas aos novos termos da legislação nacional.[20]

Em outras palavras, a LGPD “transformará o modo pelo qual as empresas e governos lidam com dados pessoais e a mudança não é pequena, envolvendo a criação de novas rotinas, de procedimentos de segurança e transparência”.[21]

O processo de Compliance à LGPD pretende, em última instância, implementar e concretizar seus conceitos e objetivos. Por definição, Compliance refere-se “ao conjunto de ações a serem adotadas no ambiente corporativo para que se reforce a anuência da empresa à legislação vigente,

---

[20] FRAZÃO, Ana; CUEVA, Ricardo Villas Boas. Compliance políticas de proteção de dados. Revista dos Tribunais, São Paulo, p. 500, 2021.

[21] VIOLA, Mário; SOUZA, Carlos Affonso; PADRAO, Vinicius. Op. Cit. P. 112.

de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno ao contexto de normalidade e legalidade"[22].

IV. A IMPORTÂNCIA DA ADEQUAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS AO COMPLIANCE NAS EMPRESAS

De acordo com o art. 50, §1º, da LGPD, ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular[23]. Logo, há a preocupação do legislador com a variedade de organizações que devem se adequar a legislação, de forma que cada uma respeite suas peculiaridades, decorrentes da característica de cada porte, tipo de atividade, dentre outros fatores que variam a cada sociedade, desde as mais simples até as mais complexas. Inclusive, segundo o art. 55-J, XVIII, da Lei Geral de Proteção de Dados, cabe à ANPD editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se à legislação.[24]

Neste diapasão, há lição de Ana Frazão, Gustavo Tepedino e Milena Donato Oliva[25]:

> "À luz do conceito de dado pessoal, até mesmo as mais simples atividades terão que se adequar à lei, vez que demandam, em alguma medida, o armazenamento de informações tuteladas pela lei – basta cogitar das informações

---

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

[23] 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: 28.07.23.

[24] Ibidem.

[25] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de Dados Pessoais**.** In**:** FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coord.) Op. Cit. p. 695.

> atinentes aos empregados ou, ainda, das listas de clientes. Mesmo operações laterais – como o que ocorre nos condomínios edilícios ao coletarem e armazenarem dados de condôminos, visitantes, funcionários – também se sujeitam à LGPD. Ressalta-se que, o programa de governança em privacidade, previsto exclusivamente para o controlador, é algo amplo, com elaboração de normas de governança corporativa. Enquanto as regras de boas práticas e governanças, tende a se preocupar com questões operacionais acerca do tratamento de dados."[26]

Nesse sentido, o programa de governança em privacidade é o conjunto de regras de boas práticas e governança a serem utilizadas pelos agentes de tratamento de dados pessoais. Como também, assemelha-se com a política de segurança da informação, mas com o objetivo de cumprir as ordens legais.[27]

Tal programa encontra-se alinhado com as políticas de governanças e compliance, que objetivam, no geral, realizar uma gestão de riscos, mediante boas práticas, observância da legislação e regulamentos internos, e criação de controles internos.[28]

O programa de compliance consiste em assegurar que o tratamento permitirá o pleno exercício de direitos dos titulares, como, por exemplo, o acesso aos seus dados. Visto que, a legislação de proteção de dados valoriza a transparência, através da participação deste.[29]

---

[26] 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. 701.

[27] BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. Lei Geral de Proteção de Dados Pessoais - LGPD. In: CARVALHO, André Castro et. al. Manual de Compliance. 2. ed. Rio de Janeiro: Forense, 2020. p. 509; COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198.

[28] COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198.

[29] FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: 56 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. 704.

Nesse sentido, Frazão, Oliva e Abílio[30], alegam que:

> "A participação do titular deverá influenciar na valoração positiva das normas de compliance pela ANPD, de modo que o envolvimento da sociedade civil na própria construção das normas corporativas e revisão da política de privacidade pode ser um relevante indício da robustez do programa."

Considerando os desafios ao desenvolvimento da governança das organizações empresariais corporativa no âmbito do cumprimento da Lei Geral de Proteção de Dados e, por conseguinte, na garantia da proteção do tratamento de dados pessoais, a Controladoria Geral da União (CGU) disponibiliza o Manual de Programa de Integridade que traz diretrizes de um programa de governança efetivo com a apresentação de cinco pilares: (i) comprometimento e apoio da alta direção; (ii) instância responsável pelo Programa de Integridade, (iii) análise de perfil de riscos; (iv) estruturação de regras e instrumentos e (v) estratégias de monitoramento continuo[31].

Dessa forma, o compliance tem como papel fazer com que as empresas atuem em conformidade com as leis, regulamentos e melhores práticas de governança corporativa, a LGPD, por outro lado, busca essa observância em relação à governança dos dados pessoais e que será alvo das operações realizadas pelas empresas.

Ademais, o compliance estabelecido e aprimorado traz grandes vantagens econômicas e reputacionais para as organizações empresariais, dentre estas vantagens estão:

> "[...] (i) vantagens reputacionais, (ii) o estímulo para maior investimento em inovação e qualidade, em razão da sua supressão dos benefícios decorrentes de vantagens ilícitas, que alteram a dinâmica concorrencial, (iii) melhorias do padrão de gestão organizacional, que podem contribuir para a eficiência da empresa, (iv) aumento das oportunidades de negócio, e, por fim, (v) a própria economia decorrente da prevenção do ilícito e/ ou da minoração de seus danos."[32]

---

[30] Ibidem, p. 705.

[31] Controladoria Geral da União. Programa de integridade: diretrizes para empresas privadas. Disponível em: [www.gov.br/cgu/.pdf]. Acesso em: 07.08.23

[32] FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Op. Cit. P. 81

Em uma pesquisa realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) ao longo do ano de 2021, com o objetivo de compreender como pequenas, médias e grandes empresas tratam os dados pessoais de seus clientes, funcionários, fornecedores e parceiros, bem como mapear as questões relevantes associadas à implementação da LGPD no Brasil, sendo um módulo específico para a produção de indicadores sobre o tema e implementado como parte do esforço de campo da pesquisa TIC Empresas 2021, os indicadores trazem um panorama amplo de práticas e mudanças organizacionais impulsionadas por esse momento inicial de aplicação da LGPD pela autoridade competente.[33]

O levantamento indica que 36% das empresas realizaram reuniões específicas para tratar do tema privacidade e proteção de dados pessoais. Ainda que não sejam observadas diferenças regionais significativas, a realização de reuniões para tratar temas relacionados à privacidade e à proteção de dados aparece de forma desigual entre os diferentes setores, sendo que os de informação e comunicação foram os que apresentaram maior frequência, e o setor de construção, a menor incidência. Ademais, vale destacar que reuniões foram mais presentes nas grandes (73%) e médias empresas (59%), enquanto nas pequenas houve uma menor proporção que buscou discutir internamente os temas de privacidade e proteção de dados pessoais.[34]

A pesquisa também traz dados sobre o público-alvo das ações de treinamento e capacitação sobre privacidade e proteção de dados pessoais ocorridos nas empresas. Em 84% das empresas que realizaram ações de treinamento, houve participação da diretoria e 85% contaram com a participação da gerência. Por sua vez, em 74% das empresas que ofereceram treinamento sobre proteção de dados houve participação de funcionários. Em menor medida, o treinamento foi oferecido aos parceiros e funcionários

[33] No marco da LGPD, foi criada a Autoridade Nacional de Proteção de Dados (ANPD), responsável pela implementação e aplicação da lei, como órgão da administração pública federal vinculado à Presidência da República. A natureza da Autoridade foi alterada para “autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal”, pela Medida Provisória n. 1.124, de 2022.

[34] Privacidade e proteção de dados pessoais 2021 [livro eletrônico]: perspectivas de indivíduos, empresas e organizações públicas no Brasil. P.75.

terceirizados, sendo destinado para os colaboradores da empresa em todos os escalões.[35]

Entre as empresas que possuem um plano de conformidade ou adequação à LGPD, a maioria das iniciativas determina as funções e responsabilidade sobre a gestão de dados pessoais na empresa (85%). Na sequência são citadas ações de conscientização e treinamento e processos para possibilitar a cooperação e troca de informação dentro da empresa (81%) — o que pode ter relações com as estratégias de capacitação discutidas acima. Portanto, as ações previstas nos planos de conformidade ou adequação à LGPD versam sobre a definição de atribuições em torno das exigências da lei, ao mesmo tempo em que há diretivas sobre capacitações internas, tanto do ponto de vista de fornecimento de conhecimentos quanto de melhoria da comunicação entre departamentos[36].

V. CONSIDERAÇÕES FINAIS

Perante o exposto, a tecnologia sempre estará em constante atualização com novas propostas e aprimoramentos para a sociedade. Consequentemente a importância de regulamentações e limitações para o manuseio e coleta dos dados é crucial. A coleta e processamento de dados ocorriam de maneira caótica e irregular, resultando em um sistema instável que se mostrou insustentável por meio das repetidas violações que se manifestaram. Essas violações não apenas afetaram a esfera da privacidade e do controle pessoal, mas também causaram interferência nos próprios processos democráticos de várias nações, como evidenciado no caso da Cambridge Analytica.

Com isso, a implementação da Lei Geral de Proteção de Dados trouxe uma transformação significativa tanto no aspecto legal quanto econômico do Brasil, marcando um ponto crucial na regulação da proteção de dados no país. Dado o amplo alcance das proteções introduzidas pela LGPD e as diversas situações em que ela é aplicada, torna-se essencial criar estratégias e

[35] Ibidem.

[36] Ibidem.

ferramentas para que as organizações implementem devidamente as diretrizes legais.

Nesse contexto, é evidente a conexão entre os princípios da LGPD e os conceitos da governança corporativa, que busca incorporar as normas estatais nos procedimentos internos das empresas. Os valores de transparência, justiça, prestação de contas e responsabilidade corporativa, que são fundamentais para a integridade empresarial, estão integralmente abordados na LGPD. A própria lei, de fato, explicitamente recomenda a adoção de boas práticas e governança como meios de efetivar e concretizar suas disposições no que diz respeito à proteção de dados. Portanto, o Compliance é aplicado de maneira apropriada para garantir a segurança e a gestão adequada dos dados pessoais.

No que se refere à gestão e à eficácia dos sistemas de integridade empresarial, é crucial que a adoção das práticas e a observância das orientações não sejam superficiais, indo além de uma mera execução mecânica de procedimentos em série. É de extrema importância estabelecer uma autêntica cultura de integridade, especialmente adaptada ao contexto de manipulação de informações pessoais, de modo a criar uma interação harmoniosa entre as diretrizes governamentais presentes na Lei Geral de Proteção de Dados e as atividades diárias das organizações.

Deste modo, a introdução da LGPD acarretou amplas transformações no contexto da salvaguarda de informações individuais no Brasil. Até que sua efetivação seja alcançada no nosso sistema legal, as organizações empresariais precisarão realizar alterações profundas na maneira como lidam com a proteção de dados. Embora haja um trajeto considerável a percorrer para estabelecer uma cultura de conformidade plena, os primeiros passos já foram tomados. Presume que as modificações trazidas pela LGPD darão origem a uma nova era de sociedade da informação no Brasil, caracterizada por cidadãos conscientizados e uma maior segurança no manejo de informações pessoais.

REFERÊNCIAS

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

BRASIL. Lei no 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, [2022] Disponível em [https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm]. Acesso em 17.05.23.

BLUM, Rita Peixoto Ferreira; MORAES, Hélio Ferreira. Lei Geral de Proteção de Dados Pessoais - LGPD. In: CARVALHO, André Castro et. al. Manual de Compliance. 2. ed. Rio de Janeiro: Forense, 2020. p. 509; COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198

CONTROLADORIA GERAL DA UNIÃO, Programas de Integridade: Diretrizes para Empresas Privadas. Brasília: CGU, 2015. Disponível em: https://www.gov.br/cgu/pt-br/centrais-de-conteudo/publicacoes/integridade/arquivos/programa-de-integridade-diretrizes-para-empresas- privadas.pdf

Compliance de dados pessoais. In.: Lei Geral de Proteção de Dados Pessoas e suas repercussões no direito brasileiro (coord. Gustavo Tepedino, Ana Frazão e Milena Donato Oliva). São Paulo: Thomson Reuters Brasil, 2019.

COTS, Márcio; OLIVEIRA, Ricardo. Lei Geral de Proteção de Dados Pessoais Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 198.

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.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. BBC. Disponível em:[https://www.bbc.com/portuguese/internacional-43461751#:~:text=A%20empresa%20não%20precisou%20%22invadir,sendo%20usadas%20para%20fins%20políticos.]. Acesso em 17.05.23

FRAZÃO, Ana; CUEVA, Ricardo Villas Boas. Compliance políticas de proteção de dados. Revista dos Tribunais, São Paulo, p. 500, 2021.

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

FRAZÃO, Ana; MEDEIROS, Ana Rafaela Martinez. Desafios para a efetividade dos programas de compliance. *In*: CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018. p. 71-104.

FRAZÃO, Ana de Oliveira. A nova Lei de Proteção de Dados Pessoais: Principais Repercussões para a Atividade Empresarial, Parte I. Disponível em: [https://www.jota.info/opinião-e-analise.] Acesso em: setembro de 2019.

GUILHERME, Luiz Fernando do Vale de Almeida. Manual de Proteção de Dados:

LGPD comentada. São Paulo: Almedina, 2021.

PINHEIRO, Patrícia Peck. Direito Digital. 6 ed. São Paulo: Saraiva, 2016.

Privacidade e proteção de dados pessoais 2021 [livro eletrônico]: perspectivas de indivíduos, empresas e organizações públicas no Brasil = Privacy and personal data protection 2021: perspectives of individuals, enterprises and public organizations in Brazil / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- São Paulo: Comitê Gestor da Internet no Brasil, 2022.

SARTORI, Ellen Carina Mattias. Privacidade e dados pessoais: a proteção contratual da personalidade do consumidor na internet. Revista de Direito Civil Contemporâneo, v. 9, ano 3, out-dez. 2016, p. 49-104.

STJ. Recurso Especial. Disponível em: [https://scon.stj.jus.br/SCON/]. Acesso em: 27.07.23

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. Lei Geral de Proteção de Dados e suas repercussões no Direito brasileiro. 2. ed. São Paulo: Revista dos Tribunais, 2020.

The world's most valuable resource is no longer oil, but data. Disponível em: [www.economist.com/leaders/2017/]. Acesso em 17.05.23.

VIOLA, Mário; SOUZA, Carlos Affonso; PADRAO, Vinicius. Op. Cit. P. 112.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, v. 30, n. 1, p. 75-89, 2015.