LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E A RELEVÂNCIA DE SUA IMPLANTAÇÃO

GENERAL PERSONAL DATA PROTECTION LAW AND THE RELEVANCE OF ITS IMPLEMENTATION

Carlos Renato Cunha[1]
Maria Amélia Barros de Albuquerque[2]
Katty Cinara Viana da Silva[3]

Como citar: CUNHA, Carlos Renato; ALBUQUERQUE, Maria Amélia Barros de; SILVA, Katty Cinara Viana da. Lei Geral de Proteção de Dados Pessoais e a relevância de sua implantação. **Revista do Instituto de Direito Constitucional e Cidadania – IDCC**, Londrina, v. 8, n. 1, e078, jan./jun., 2023. DOI: 10.48159/revistadoidcc.v8n1.e078

Resumo: O presente estudo pretende demonstrar a relevância da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) às pessoas físicas e jurídicas, diante do atual cenário da tecnologia da informação e sua importância para a sociedade, e a atuação do poder público no tratamento de dados pessoais, em razão de sua atividade estatal. Para tanto, a contextualização dos aspectos gerais apresentados na Lei nº 13.709/2018, a construção histórica da política de proteção de dados, por meio das leis que a antecederam e serviram de base para sua criação, bem como os fundamentos e princípios nela apresentados, são elementos significativos para a tarefa hermenêutica sobre o texto da lei a fim de verificar a relevância de sua aplicação pelos agentes públicos e privados. Assim, por meio do método dedutivo e da pesquisa bibliográfica, faz-se necessário debruçar sobre os limites e as garantias encontradas na sua implantação, salientando as dificuldades e os benefícios da aplicação da LGPD e considerando o ponto de vista do Fisco e do contribuinte. Conclui-se que, apesar de muitos aspectos ainda necessitarem de amadurecimento na aplicação da política nacional de proteção de dados pessoais, e ainda, uma regulamentação mais eficaz e orientação mais ativa dos órgãos responsáveis, a fim de que atenda a sua finalidade e integrem todos os agentes que participam da relação de tratamento de dados pessoais, a LGPD é indispensável à economia dos negócios em uma era digital, à privacidade, à intimidade, à dignidade da pessoa humana, à democracia, e acima de tudo, aos preceitos do Estado Democrático de Direito.

Palavras-chave: LGDP; Tecnologia; Informação; Dados Pessoais; Empresa; Contribuinte.

Abstract: The present study intends to demonstrate the relevance of the application of the General Law for the Protection of Personal Data (LGPD) to individuals and legal entities, given the current scenario of information technology and its importance for society, and the performance of the public power in the treatment of personal data, due to state activity. Therefore, the contextualization of the general aspects presented in Law nº 13.709/2018, the historical construction of the data protection policy, through the laws that preceded it and served as the basis for its creation, as well as the fundamentals and principles presented therein, are significant elements for the hermeneutic task on the text of the law to verify the relevance of its application by public and private agents. Thus, through the deductive method and bibliographical research, it is necessary to investigate the limits and guarantees found in its implementation, highlighting the difficulties and benefits of applying the LGPD and considering the point of view of the Tax Authorities and the taxpayer. It is concluded that, although many aspects still need to mature in the application of the national policy for the protection of personal data, and also, a more effective regulation and more active guidance of the responsible bodies, so that it meets its purpose and integrates all agents who participate in the personal data processing relationship, the LGPD is indispensable to the economy of business in a digital age, privacy, intimacy, human dignity, democracy, and above all, the precepts of the Democratic State.

Keywords: GDPL; Technology; Information; Personal Data; Society; Taxpayer.

1 Doutor em Direito do Estado pela Universidade Federal do Paraná - UFPR (2019). Mestre em Direito do Estado pela UFPR (2010). Especialista em Planejamento Tributário e Operações Societárias pela Faculdade Brasileira de Tributação - FBT (2015). Especialista em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários - IBET (2005). Bacharel em Direito, pela Universidade Estadual de Londrina (2002). Procurador do Município de Londrina (PR) desde 2004. Professor do Mestrado Profissional em Direito, Sociedade e Tecnologias da Escola de Direito das Faculdades Londrina. Professor da Graduação em Direito na Pontifícia Universidade Católica - PUC-PR, Campus Londrina (PR). Professor da Graduação em Direito nas Faculdades Londrina, em Londrina (PR). Professor da Pós-Graduação "lato sensu" em Direito em diversas instituições, atuando como Professor Conferencista do IBET. Coordenador do grupo de pesquisa em "Tributação, Eficiência e Direitos Fundamentais da PUC/PR Campus Londrina. Coordenador do Curso de Especialização em Direito Tributário, Compliance e Planejamento Fiscal da PUCPR Campus Londrina. E-mail: carlosrenato80@gmail.com.

2 Mestre em Direito, Sociedade e Tecnologias nas Faculdades Londrina (PR). Especialista em Direito Tributário pelo Instituto Brasileiro de Estudos Tributários – IBET. Advogada. E-mail: maria.amelia@balera.com.br.

3 Especialista em Direito Aplicado pela EMAP. Graduada pela UEL. Assistente II de Juiz de Direito da Região Metropolitana de Londrina - Foro Regional de Rolândia. E-mail: kattycinara@hotmail.com.

1. INTRODUÇÃO

Com os grandes avanços tecnológicos, por meio do crescimento significativo de acesso à internet de banda larga pela população mundial e difusão da telefonia móvel, e a partir da transformação digital, surgiram novos desafios para a atuação estatal nos direitos e garantias fundamentais, especialmente, no que se refere ao enfrentamento do agravamento do princípio da vulnerabilidade dos consumidores digitais. De um modo geral, a transformação digital trouxe melhorias na condição de vida, mas também riscos para o bem-estar dos indivíduos e para a preservação de uma sociedade justa.

Nesse sentido, "a globalização é ainda um jogo sem regras; uma partida disputada sem arbitragem, onde só os gigantes, os grandes quadros da economia mundial, auferem as maiores vantagens e padecem os menores sacrifícios" (Bonavides, 2001, p. 139). Surge então, a necessidade de assegurar aos cidadãos padrões mínimos e inderrogáveis de proteção no ciberespaço.

Ademais, neste novo modelo da era digital, outra forte preocupação é com a privacidade, vez que os dados pessoais passaram a ocupar um lugar de destaque na sociedade, em razão do seu valor econômico e por ser um grande aliado para as organizações públicas e privadas obterem vantagens políticas, econômicas, pecuniárias, dentre outras. Desta forma, em razão do aumento da quantidade de dados e o fácil acesso às informações, temos uma redução no controle das pessoas sobre a utilização de seus dados, constituindo uma assimetria informacional, ou seja, "é a descrição de um fenômeno segundo o qual alguns agentes econômicos têm mais informações do que outros" (Redecker, 2021, p.1).

E dentro deste cenário de desenvolvimento e contínuo emprego das tecnologias digitais, o ordenamento jurídico brasileiro migrou para uma atuação mais ativa na proteção dos dados pessoais. Inicialmente, a privacidade e a proteção de dados eram contempladas em dispositivos da Constituição Federal de 1988, no Código de Defesa do Consumidor de 1990 (Lei nº 8078/90), na Lei de Acesso à Informação (Lei nº 12.527/2011), Lei do Cadastro Positivo (Lei nº 12.414/2011), Marco Civil da Internet (Lei nº 12.965/2014), dentre outras decisões judiciais. Mas, foi somente com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, que o sistema jurídico brasileiro supriu uma lacuna e buscou uniformizar as decisões em relação a dar proteção à privacidade e aos dados pessoais das pessoas naturais, bem como conferir aos seus titulares poder de decisão diante de seus dados.

Em âmbito internacional, o caso *Cambridge Analytica* que veio a público em 2018, demonstrou claramente a necessidade de uma política que regulamentasse a proteção de dados pessoais e impedisse o compartilhamento indevido desses dados. Esse acontecimento, influenciou diretamente a criação da Lei Geral de Proteção de Dados no Brasil. Outra forte influência recebida pela LGPD, foi a *General Data Protection Regulation* (GDPR), do direito europeu.

Com essas mudanças no cenário mundial e interno referentes ao direito digital, especificamente, na proteção de dados pessoais, a lei trouxe maior segurança jurídica para as relações estabelecidas por meio virtual com a regulamentação na forma do tratamento de dados, os limites à esses acessos e os princípios a serem observados, ou seja, *a) finalidade; b) adequação; c) necessidade; d) livre acesso; e) transparência; f) segurança; g) prevenção; h) não discriminação; i) qualidade dos dados; j) responsabilidade e prestação de contas* (art.6º).

Neste contexto, expõe Pinheiro (2021, p. 79) a respeito:

> Nota-se que o principal objetivo da lei foi a atualização dos mecanismos regulatórios do país frente às necessidades surgidas com o desenvolvimento e expansão da tecnologia e aumento cada vez mais expressivo da coleta, processamento, transmissão e armazenamento de dados no ambiente virtual.

Assim, umas das inovações da LGPD foi a imposição de obrigações e deveres aos agentes de tratamentos para adotarem melhores práticas e procedimentos razoáveis de prevenção de incidentes de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados (art. 50), sob pena de serem responsabilizados pela reparação dos danos (art. 42). Assim, os agentes de tratamento poderão ser sujeitos às sanções administrativas, previstas no rol do art. 52, aplicáveis pela ANPD (Autoridade Nacional de Proteção de Dados), sem prejuízo de responsabilização civil pelo titular de dados perante o Poder Judiciário. Em relação ao poder público, o art. 23 dispôs que o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá observar a sua finalidade pública, no interesse público, dentro de suas competências legais ou atribuições legais do serviço público.

Com isso, parece-nos essencial e pertinente analisarmos as dificuldades e benefícios na implantação da lei tanto do ponto de vista das pessoas naturais como das pessoas jurídicas.

Para tanto, abordaremos, inicialmente, uma breve análise histórica do seu surgimento. Após essas considerações, apresentaremos os aspectos gerais, os objetivos e os princípios da lei de proteção de dados, e desde já, destacando que a LGPD é uma lei, predominantemente, principiológica, e, por fim, analisaremos os pontos negativos e positivos na implantação da citada lei, tanto do ponto de vista das pessoas naturais como das pessoas jurídicas, sob a

perspectiva tributária, demonstrando que a necessidade de regulamentação do tratamento de dados supera quaisquer empecilhos que possam se apresentar.

2 DIREITO, TECNOLOGIA E PROTEÇÃO DE DADOS: ASPECTOS GERAIS DA LGPD

2.1 POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS E SUA CONSTRUÇÃO HISTÓRICA

O uso crescente das tecnologias de comunicação e informação, por meio da internet, de aplicativos, entre outros meios digitais, na oferta ou na aquisição de bens e serviços, nas relações interpessoais, jurídicas, comerciais ou sociais, foi incorporado ao cotidiano das pessoas possibilitando conversas, compras e vendas, reuniões, pesquisas, atendimentos médicos, aulas, palestras, lançamentos de tributos e uma série de outras atividades, exclusivamente pelo meio virtual.

Assim, com a evolução tecnológica, houve um crescimento exponencial da informação, e, paralelamente uma preocupação com a privacidade, pois "os dados pessoais passaram a obter um valor econômico e a servir como ferramenta para as organizações públicas e privadas para angariar vantagens pecuniárias, políticas, dentre outras." (Redecker, 2021, p. 1).

E para acompanhar esse fenômeno social, a proteção aos dados pessoais, inclusive nos meios digitais, foi incluída no rol de direitos fundamentais do artigo 5º da Constituição Federal: "*LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Incluído pela Emenda Constitucional nº 115, de 2022)*" (Brasil, 1988).

Segundo dados divulgados pela pesquisa TIC Domicílios, realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), houve um aumento significativo do uso da Internet em 2020 no Brasil: se antes 74% (setenta e quatro por cento) da população estava conectada, o acesso naquele ano passou a ser de 81% (oitenta e um por cento) da população, o que representou, aproximadamente, 152% (cento e cinquenta e dois milhões) de pessoas plugadas pelos diversos meios possíveis à Internet – computadores, tablets, celulares, etc. [1]

O aceleramento do uso dos meios digitais se deu, sobremaneira, pelo assolamento da pandemia do COVID. As pessoas, repentinamente, se viram em suas casas, com suas

[1] G1. **Uso da internet no Brasil cresce, e chega a 81% da população, diz pesquisa**. G1 – Economia, Tecnologia**.** 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/08/18/uso-da-internet-no-brasil-cresce-e-chega-a-81percent-da-populacao-diz-pesquisa.ghtml. Acesso em: 03 ago. 2022.

necessidades físicas continuadas, mas agora, restritas, sem poderem sair. Fez-se necessário mudar os rumos do consumo, mudar o rumo das relações interpessoais e de trabalho.

No entanto, com esta nova realidade e a ampliação da abrangência da conectividade e, de certa forma, do olhar de "vida", surgem também situações de conflito, violação de direitos e deveres, incluindo o mau uso do meio virtual[2]. E isso, implicou na necessidade de adaptação e colaboração da sociedade como um todo, para amparar os casos de violações e transgressões.

E é neste contexto que o Direito Digital nasce, como resposta às demandas decorrentes do uso - e principalmente do mal-uso - de tecnologias e *internet* nas comunicações interpessoais e entre os cidadãos/contribuintes e o Estado constitucionalmente erigido.

Assim, temos que o Direito, enquanto ciência jurídica que tutela as relações sociais por meio de regras e normas, tem o dever de adentrar ao ramo digital para disciplinar e corresponder aos novos desafios da atualidade a fim de proteger os direitos e deveres da sociedade. Em relação ao elencado, Araújo (2017, p. 127) descreve:

> A doutrina tem assinalado um aspecto interessante desse ramo do Direito: afirma que o Direito Digital não tem objetivo próprio. Seria um Direito com um "modus operandi" diferente, sendo, na verdade, a extensão de diversos ramos da ciência jurídica, que cria novos instrumentos para atender a anseios e ao aperfeiçoamento dos institutos jurídicos em vigor.

Esse novo ramo do Direito vem para tutelar aquilo que não está posto, mas que tem urgência em ser tutelado, porque já está latente e urge em direitos e deveres, violações e transgressões. A tecnologia desenvolve-se em uma velocidade anos-luz da atuação Estado-lei, entretanto, o direito necessita acompanhar essas transformações nas relações sociais, no meio digital, criando regramento próprio, com suas premissas, limitações, garantias, princípios e tratamento.

Assim, no âmbito internacional, em 2016, a proteção de dados pessoais tomou novas roupagens com o advento da General Data Protection Regulation (GDPR), publicada pela Uniao Europeia, norma obrigatória que abrange todas as empresas que manipulam dados pessoais de cidadãos europeus, independentemente do local de sua sede. A referida lei funda-se no consentimento do titular que outorga ou desautoriza a qualquer tempo sua concessão, a partir de um conhecimento claro do motivo da utilização do dado pessoal pela empresa coletora. Desse modo, tem-se de forma clara que para a lei europeia a motivação do uso das informações

[2] Idem. Acesso em: 03 ago. 2022.

e dados precisa ser de conhecimento do titular para que tenha seu consentimento e, assim, possa ser usado por outrem a partir de sua ordem de vontade (Pimentel, 2018).

Após dois anos da entrada em vigor da regulamentação europeia, em 2018, a legislação brasileira aprovou uma lei específica no tratamento de dados pessoais. Essa foi inspirada precipuamente e sobremaneira na legislação europeia e trouxe de forma clara as veias das garantias no país.

Surge então, a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD), como desdobramento do Direito Digital, uma vez que vem tutelar os direitos e garantias constitucionais, tais como a vida privada, a intimidade, a honra, a imagem, a utilização e/ou divulgação indevida de informações e dados pessoais das pessoas naturais.

Temos um grande avanço em nossa sociedade e devemos encarar com bons olhos esse passo dado em direção à garantia dos direitos socioeconômicos, uma vez que o objetivo da normativa é a maior transparência e padronização na interação digital, proporcionando segurança nas relações e proteção do direito constitucional da liberdade e intimidade, reafirmando o livre desenvolvimento da personalidade da pessoa humana.

A LGPD dispõe sobre o tratamento de dados obtidos por pessoas físicas ou jurídicas, de direito privado ou de direito público, garantindo proteção e amparo ao titular da informação, impedindo que outrem se utilize desses dados de maneira inadequada ou não autorizada.

Com efeito, a lei permite que o titular decida o que será feito com a sua informação/dado a partir do direito de conhecer quem o detém, quem o utilizará e de que modo o fará. Reitera-se aqui, data vênia, a maestria desta lei que não só trouxe avanços, mas concretizou e perpetrou garantias necessárias ao nosso ambiente cibernético-constitucional.

Insta mencionar o Marco Civil da Internet, Lei nº 12.965, publicada em 2014, que estabeleceu princípios, garantias, direitos e deveres para usuários da internet no Brasil e baseou-se na neutralidade da rede, liberdade de expressão e privacidade dos usuários, servindo de premissa para a LGPD (Netto, 2022).

Anteriormente, o Brasil não tinha normas significativas que regulamentasse às relações na Internet, mas já tinha uma infinidade de relações acontecendo no universo digital. Portanto, era necessário um instrumento regulamentador que trouxesse o mínimo, e foi esse o papel do Marco Civil da Internet. A Lei nº 12.965/2014 surgiu em uma fase em que as relações entre os sujeitos de direito no mundo cibernético já aconteciam intensamente, mas o Brasil não havia quase nada que regulamentasse esse intercâmbio de informações e troca de dados. Assim, foi

importante para começar um universo de princípios e normas e nortear as diretrizes regulamentadoras do Direito Digital.

Cita-se alguns dos conceitos postos pelo Marco Civil da Internet que foram importantes para a construção do universo jurídico que se tem hoje sobre Direito Digital. Por neutralidade, entendeu-se a rede com transporte de dados com o impedimento de discriminações tangentes à natureza do conteúdo ou à identidade do usuário; por liberdade de expressão, entendeu-se a permissão ao usuário de manifestar-se livremente quanto a opiniões, pensamentos etc.; e, por privacidade, pode-se entender a barreira à divulgação de dados, informações pessoais, bem como o controle desses dados por pessoa não autorizada. Desses três pilares, a liberdade de expressão foi destacada na Lei com o intuito de impedir qualquer tipo de censura no âmbito digital (Teffé; Moraes, 2017).

Embora alguns doutrinadores critiquem a criação da Lei nº 12.965/2014 atacando-a sob o prisma de não possuir eficácia normativa, não trazendo soluções concretas às dificuldades enfrentadas pelas atuais relações virtuais (Tomasevicius Filho, 2016), faz-se necessário salientar que o Marco Civil da Internet aconteceu em um momento enigmático, conforme já citado, em que as relações no mundo cibernético já aconteciam em escalas acentuadas, mas não existiam instrumentos normativos que as regulamentassem.

A Lei nº 12.965/2014 abriu espaço para que após sua edição outras normativas despontassem objetivando resguardar de maneira mais específica alguns aspectos relevantes das relações cibernéticas e, por essa razão, deve ser analisada sob a ótica do impulso à normatização dos usuários da internet e não como meramente especuladora do Direito Digital.

Por fim, para concluir a análise histórica da Lei Geral de Proteção de Dados Pessoais, vale sintetizar um escândalo que se tornou conhecido em 2018 pelo vazamento de dados pessoais, e que demonstra de modo inequívoco a importância de uma lei regulamentadora no tratamento de dados pessoais: o caso Cambridge Analytica.

A empresa britânica Cambridge Analytica trabalha com mineração e publicidade estratégica de massa de dados, mais conhecida como *big data*, para traçar perfis de consumidores e eleitores objetivando o envio de propaganda mais direcionada conforme os perfis dos usuários analisados e catalogados em consonância a logaritmos (Netto, 2022). Desta forma, a empresa analisa os perfis em específico e direciona a propaganda de forma que a propaganda seja recepcionada por aqueles que realmente tenham interesse naquele assunto. É a chamada mineração.

Neste contexto, chegou ao conhecimento público, em 17 de março de 2018, por meio de uma reportagem da TV Channel 4, que a empresa teve acesso à dados de mais de 87 (oitenta e sete) milhões de usuários do Facebook coletados no ano 2014, época em que o Facebook permitia que aplicativos extraíssem informações de seus usuários sem grandes (ou quase nenhum) filtro, e utilizou-os para influenciar eleições em inúmeros países democráticos nos mais diversos continentes, ou seja, a empresa Cambridge Analytica coletou os dados dos usuários e direcionou propaganda aos redutos eleitorais direcionados, fazendo com que eleições no mundo todo fossem maquiadas, ou, melhor dizendo, direcionadas (Netto, 2022).

O caso tomou grandes proporções pois envolvia países com economias mundiais significativas, que tiveram suas eleições maquiadas e conduzidas por dados supersensíveis. Esses foram monitorados e utilizados a partir de troca de informações dos usuários nas redes sociais sem que os usuários tivessem o conhecimento de que estes dados estivessem sendo utilizados com os fins para os quais foram utilizados.

Sabe-se que os dados na época utilizados não foram apenas do Facebook, mas também de outras redes sociais importantes e com potenciais e significativas colocações no mercado, como Instagram, Twitter, Google e até WhatsApp de mais de 50 (cinquenta) milhões de usuários (Netto, 2022). Em relação aos dados do WhatsApp, que são mega sensíveis, as chamadas *big datas* oferecem dinheiro para comprar informações dos grupos de amigos e de família para saber as tendências políticas e os assuntos mais falados, e assim catalogam o que se está sendo falado ao longo de um país em ambientes considerados superprivados.

Na época, a justificativa foi que os dados e informações coletadas eram para fins acadêmicos, de pesquisa e estudo; algo utilizado sem qualquer motivação política e/ou econômica, financeira. No entanto, as investigações demonstraram que houve a criação de um algoritmo com o objetivo do cruzamento das informações para criar um perfil orgânico de cada cidadão, individualmente considerado, em um primeiro momento, e em seguida, catalogando este cidadão a subgrupos, a grupos específicos e ainda a um grupo maior e com grande potencial econômico: o eleitoral.

O caso Cambridge Analytica tornou-se um escândalo global. Entretanto, a reflexão que deixou ao mundo foi quanto a privacidade e intimidade de usuários da Internet podem ser violadas pelo uso das redes sociais e pela navegação em sites que permitem a captação de dados sensíveis e quanto isso fere não só os direitos dos titulares das informações, mas da sociedade como um todo que, direta e indiretamente, sofre as consequências das manipulações com

resultados intermediados e/ou vendidos e/ou maquiados. O vazamento de dados pessoais é um verdadeiro ataque à democracia e à sociedade contemporânea.

2.2 PRINCÍPIOS E FUNDAMENTOS DA LGPD

No atual contexto social, que a fragilidade e a sensibilidade dos dados pessoais estão escancaradas, principalmente, no meio virtual, a necessidade de intervenção do direito, por meio de regulamentação da utilização e divulgação dos dados pessoais, tornar-se uma ferramenta indispensável para proteger o seu titular e amenizar os danos do seu uso indevido.

Assim, compreender os fundamentos e os princípios elegidos pela lei de proteção dos dados pessoais, é a principal tarefa para dar segurança e eficiência no tratamento desses dados, a fim de atingir o seu objetivo. Além disso, o cientista do direito, tem o dever de realizar essa análise hermenêutica de forma sistêmica, considerando o ordenamento jurídico a qual ela está inserida, dialogando com as outras fontes normativas, e axiológica, atribuindo-lhe o seu valor, a partir de sua natureza e classificação.

Nesta perspectiva, a LGPD inicia-se apresentando seu objetivo, que é a disposição sobre o tratamento dos dados das pessoas naturais. Neste sentido, a lei faz uma ressalva extremamente relevante e integrativa ao elencar que dispõe sobre os dados pessoais *inclusive nos meios digitais* (art.1º). Isso porque seu foco principal é a proteção das informações que são transmitidas pela Internet (e outros meios digitais). E cabe aqui salientar que, isto não exclui a proteção dos dados pessoais transmitidos e/ou operados por meios físicos.

Seguindo a narrativa, a lei trata sobre a proteção dos direitos fundamentais de liberdade, de privacidade e de desenvolvimento da personalidade de pessoas naturais a partir do tratamento de dados por pessoas naturais ou jurídicas. Neste sentido, importante ressaltar que a lei exclui de sua apreciação os dados utilizados por pessoas naturais unicamente com fins privados e sem destinação econômica - o fim deve ser, *in casu*, a finalidade da manipulação dos dados com o objetivo de tirar um proveito lucrativo disso, bem como também não considera os dados quando são usados para fins jornalísticos, artísticos ou acadêmicos/estudos de qualquer natureza e, ainda, com fins de proteção à segurança pública ou do Estado, defesa nacional ou investigação criminal (art. 4º).

No tocante a segurança pública ou do Estado, defesa nacional e investigação criminal, a LGPD determina que legislação específica tratará desses casos (art. 4º, §1), o que demonstra à lei grande preocupação, a fim de evitar que pessoas de direito privado fiquem responsáveis

pelo tratamento dos dados sensíveis, exceto em situações em que o Poder Público exerce supervisão extensiva (Pimentel, 2018).

Os fundamentos salvaguardados no segundo artigo da legislação, que trouxe a proteção ao que chamamos de era digital, foram a privacidade, a autodeterminação informativa, a liberdade de expressão, a liberdade de comunicação, de opinião e de informação, a inviolabilidade da intimidade, da honra e da imagem, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e exercício de cidadania.

Conforme se denota, todos os direitos individuais devem ser interpretados pela égide da proteção de dados, ou seja, a partir da conferência ao titular da informação em publicar e dispor de sua imagem, gostos, pensamentos, opiniões etc. da forma como desejar. Além disso, este tem esse direito integralmente considerado contra terceiros com o intuito de utilizarem essas informações sem o seu consentimento e/ou utilizarem para fins diferentes ou discrepantes do autorizado por aquele que foi o emissor do dado ou informação sensível (Garcia et al., 2020).

Os demais fundamentos constantes no artigo 2°, como desenvolvimento econômico, tecnológico e inovação, livre iniciativa, livre concorrência e defesa do consumidor, dizem respeito não só aos indivíduos de modo particular, mas abrangem também o desenvolvimento da sociedade de forma holística.

Nas palavras de Garcia et al. (2020, p. 90) temos:

> Nestes casos, a interpretação cabível é o reconhecimento do legislador da importância dos dados na sociedade da informação e do conhecimento. Embora o dado isolado não agregue valor, ele é fundamental quando analisado conjuntamente, em um contexto, com objetivos e finalidade. Assim, o dado passa a ser informação capaz de ser suporte para a tomada de decisões sociais, políticas e econômicas, especialmente neste último caso, como motor econômico da livre iniciativa e alavanca para a inovação e tecnologia, sem, contudo, deixar de lado a defesa do consumidor.

Com efeito, o artigo 2° demonstra a preocupação do legislador em proteger a pessoa natural tanto em sua esfera privada, como consumerista e contributiva - holística, sem se descuidar do desenvolvimento econômico e social que depende do recurso da informação para sua tomada de decisões. A lei tem como objetivo resguardar a proteção dos resultados que sobrevierem no meio digital e físico, ressalvando sobremaneira as conjecturas do meio em que ocorreu.

Já em relação à sua aplicabilidade, a lei se restringe ao território nacional e aos dados cujo tratamento sejam provenientes do Brasil ou que sejam objeto de compartilhamento, comunicação ou transferência com agentes brasileiros. Assim, se expressa a importância para a lei nacional, de que os dados sensíveis sejam tratados no Brasil e que tenham como destino e

a finalidade, organicamente considerada, a nação brasileira enquanto forma, operação e atividade de tratamento (art. 3º).

Além disso, a Lei Geral de Proteção de Dados conceitua uma série de termos que são importantes para o entendimento do objeto ao qual ela se destina (art. 5º). O primeiro destacado é o dado pessoal sensível, como o dado que contém informações quanto à raça, religião, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, referente à saúde ou vida sexual, dado genético ou biométrico. São os dados considerados mínimos do cidadão e que somente a ele dizem respeito por isso intitulado de dados pessoais sensíveis.

Titular é definido como a pessoa natural a quem se referem os dados, ou seja, aquele de quem se fala ou aquele de quem se refere ou se faz a referência. O controlador é citado como o agente responsável pelas decisões referentes ao tratamento dos dados. A lei cita em vários pontos o controlador e ele se mostrará uma figura importante pois está diretamente ligado ao tratamento das informações em referência. Neste mesmo sentido, a legislação traz a figura do operador como aquele que realiza o tratamento por comando do controlador. Assim, tem-se um sujeito, o controlador, que dá ordens ao operador, para que este faça ações com o objetivo de preservar ou tratar as informações objeto da intervenção.

Outra novidade da Lei Geral de Proteção de Dados Pessoais é a figura do encarregado, uma pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). E entre as suas atribuições, definidas pela lei, estão as de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências; receber comunicações da autoridade nacional e adotar providências; orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares. Frisa-se que a autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições dos encarregados (art. 41).

Em seu art. 6º, a Lei Geral de Proteção de Dados Pessoais, elenca os princípios que devem ser observados no tratamento dos dados, precipuamente, a boa-fé, bem como a finalidade do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular; adequação, ou seja, a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; necessidade, consistente em 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;

livre acesso aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; qualidade dos dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; transparência 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; segurança mediante a 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; prevenção, com a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; não discriminação, vedado a realização do tratamento para fins discriminatórios ilícitos ou abusivos; e por fim, a responsabilização e prestação de contas 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.

Salienta-se que esse rol não é taxativo, a par de outros que visam a responsabilidade por parte do controlador e operador dos dados e a clareza do titular em relação ao destino e motivação no tratamento de seus dados (Garcia et al., 2020).

No mais, extrai-se da lei que, o tratamento de dados pessoais necessita do consentimento do titular (art. 7º, I), sendo este dispensado apenas em casos específicos, tal como dados que sejam tornados públicos pelo titular por sua manifestação de vontade e, mesmo nesses casos, o controlador deve observar os princípios e resguardar os direitos do titular (art. 7º, §4º). Ressalta-se que se os dados tratados forem sensíveis, mais rigorosa a restrição da lei quanto a dispensa de autorização (art. 11).

Outro caso de dispensa do consentimento do titular, são os dados pessoais tratados pela Administração Pública e o seu compartilhamento por medidas necessárias à execução de políticas públicas previstas em leis ou regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (art. 7º, III).

O regramento do tratamento de dados pessoais pelo poder público está previsto no Capítulo IV da Lei 13.709/2018 e se justifica no atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público (art. 23). Para tanto, o poder público deverá observar, cumulativamente, (I) que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a

execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; (II) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais;

A legislação também dispõe do tratamento quando realizado pelo Poder Público, da responsabilidade dos agentes de tratamento e da boas práticas e segurança genericamente considerada (art. 32).

O art. 18 prever que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a confirmação da existência de tratamento, o acesso aos dados, a correção de dados incompletos, inexatos ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei, a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial, a eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei, a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, a informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

A partir da enumeração cadenciada dos direitos do titular dos dados, transparece uma sequência de obrigações do controlador que para fazer face às exigências legais do titular deve estar preparado para cumpri-las sempre que requisitado. Nas palavras de Peloso Piurcosky et al. (2019, p. 90), “A LGPD deixa claro que os titulares dos dados têm total direito sobre suas informações, dando a eles mais controle e, às empresas, responsabilidades”.

Ademais, o artigo 20 da lei aborda a questão da solicitação pelo titular da revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais e que afetem seus interesses, tais como as que definem o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade, determinando o § 1º que o controlador deverá fornecer essas informações de maneira clara e adequada, sempre que forem solicitadas, devendo respeitar os segredos comerciais e industriais. Já o § 2º, por seu turno, elenca que em caso de não oferecimento de informações de que trata o § 1º, baseado na sincronicidade dos segredos elencados, a autoridade nacional poderá realizar uma séria de auditorias para investigação de feitios discriminatórios no tratamento automatizado de dados pessoais em referência.

A LGPD ainda disciplina como os dados pessoais de crianças e adolescentes devem ser tratados, e traz algumas especificidades, uma vez que as informações são sensíveis e tratam de pessoas jurídicas e biologicamente ainda mais frágeis e indefesas (art. 14).

O Capítulo VI da Lei dedica-se aos agentes de tratamento de dados. Em sua seção I, destaca que o controlador e o operador devem manter o registro das operações por eles realizadas precipuamente quando estes tiverem interesse nestas ações (artigo 37).

O segredo comercial e industrial também foram objeto da legislação, de forma que a autoridade nacional poderá determinar ao controlador que elabore relatório que assevere os impactos à proteção dos dados pessoais, resguardando o segredo comercial e industrial (artigo 38), assunto citado reflexivamente pela lei anteriormente.

Ainda importante ressaltar a forma como a LGPD dispõe a maneira que o operador deverá tratar as informações, ou seja, deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria (art. 39).

Desse modo entende-se que ficará a critério do controlador o estudo e cientificação das especificações acerca da matéria em referência para alinhamento com o operador. Na sequência, o artigo 41 destaca que ficará a critério do controlador a indicação de quem será o encarregado. Com efeito, dentre essas regulamentações pode-se avultar a questão da responsabilidade dos agentes de tratamento deixando a Lei às claras de que não se trata de obrigação meramente moral, mas com consequências legais bem definidas no caso de descumprimento das especificações no tratamento de dados pessoais.

Nunes (2021, p. 51) expõe sobre a temática acima de maneira bastante assertiva:

> Como se vê, a LGPD não específica de forma clara e objetiva todos os atos de um procedimento a ser percorrido pelos agentes de tratamento rumo à adequação. Preferiu o legislador apenas estabelecer a natureza das medidas que devem ser adotadas, assim como as finalidades que devem alcançadas pela adoção das referidas medidas, recomendando que os sistemas utilizados obedeçam a padrões de boas práticas e de governança. Isso faz todo sentido, pois há que se considerar na implementação da lei a realidade de cada organização destinatária, seu ramo de atividade, modelo de negócio, os processos utilizados no tratamento de dados pessoais, a importância destes para o desenvolvimento e incremento do negócio. Assim sendo, o caminho que cada organização decidirá percorrer para atender e se adequar à lei poderá variar, desde que sejam alcançados os objetivos de garantir a privacidade, a liberdade, e o livre desenvolvimento da personalidade da pessoa natural, por meio da proteção dos seus dados pessoais.

Segundo Nunes (2021), a lei não teria sido direta e objetiva em elencar o procedimento a ser seguido pelos agentes em caso de violações, mas apenas teria dado os caminhos que deverão ser percorridos por eles nos casos de se depararem com uma transgressão. Ao concluir seu raciocínio, diz que o legislador teria sido assertivo, pois cada entidade sabe o caminho que irá percorrer para atender e se adequar às exigências da Lei – como fará para conseguir colocar em prática tudo o que ele exige em questão de valores e em questão de vida prática, ações.

Desta maneira, se por um lado a lei deixa evidente a obrigação de adequar-se as normas e as consequências de sua não observância, por outro, abre espaço para que os controladores e operadores de dados pessoais desenvolvam métodos e técnicas próprias de acordo com suas possibilidades para atingir os objetivos legais. Essa abertura de possibilidades é a brecha usada para as empresas se utilizarem de um ou de outro método com o objetivo de se adequarem ao que o legislador dispôs como exigência legal.

A LGPD determina de forma objetiva que toda empresa implemente um programa de Governança de dados que esteja estruturado e arraigado junto ao seu fluxo operacional, qual seja, a rotina da empresa (art. 50). Com efeito, a normativa cria ainda uma autarquia especial dotada de autonomia técnica e decisória vinculada a Presidência da República: a Autoridade Nacional de Proteção de Dados (ANPD) cujo objetivo é fazer cumprir as determinações da LGPD em suas especificidades e normatizações, contando com o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade para auxiliá-la nestas tarefas e finalidades.

E, por fim, a fiscalização, abordada no art. 52, implica em advertência, multa simples e multa diária, sendo que a multa simples pode chegar até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração, publicização do ocorrido após confirmação da infração, bloqueio e eliminação de dados a que se refere a infração, suspensão parcial do banco de dados ou da atividade de tratamento por período máximo de 6 (seis) meses e proibição do exercício da atividade de tratamento de dados.

Insta ressaltar que o disposto no artigo acima não substitui a aplicação de sanções administrativas, civis ou penais. As sanções mencionadas são aplicadas aos infratores após confirmação por processo administrativo com direito a ampla defesa. Com efeito, tem-se que todos os direitos constitucionalmente erigidos serão garantidos num eventual processo para aferição de responsabilidade por infração no caso de lesão decorrente do mau uso do ambiente cibernético.

2.3 DIFICULDADES NA IMPLANTAÇÃO DA LGPD

Conforme exposto acima, as infrações decorrentes da violação das normas de proteção de dados são bastante severas e podem ser indicadas como a maior preocupação para as transgressões realizadas às empresas. Assim não poderia ser diferente. O mundo cibernético brasileiro, consoante já enfocado, estava à deriva e sedento por limitações e normativas. Após o tão conturbado período de *vacacio legis*, a LGPD entrou em vigor, finalmente, em setembro de 2020 e manteve as infrações penais suspensas passando estas a vigorar tão-somente em agosto de 2021.

Isso aconteceu uma vez que o legislador considerou que a sociedade não estava pronta para a implementação da norma e, por isso, teria um período maior de preparação para colocar as exigências em prática para, somente após o período indicado, vir a ser sancionada pela transgressão dos dispositivos elencados pela LGPD. As empresas tiveram mais um momento para se adaptarem a tudo o que foi disposto, desembolsarem quantias (algumas vezes espantosas) para se adaptarem às exigências e, só depois disso, passarem a ser penalizadas pelo eventual e factível descumprimento pela não implementação das exigências trazidas pela norma regulamentadora.

Como vimos no capítulo acima, diversas foram as requisições dispostas pela LGPD para que as empresas se adaptassem e fizessem suas alterações e mudanças para que ficassem em consonância aos ditames legais e, sobremaneira, houvesse uma mudança de cultura a fim de que a proteção dos dados pessoais passasse a ser elementar em todo e qualquer processo.

Tem-se, portanto, a instituição de uma nova cultura de privacidade e proteção às informações pessoais, aplicada tanto aos titulares de dados "que passam a se tornar mais conscientes e educados acerca de seus direitos e posturas ideais", quanto às organizações, "que passam a ter acesso a regra mais claras sobre como realizar o manuseio dos dados pessoais de forma ética e coerente" (Pinheiro; Lotufo, 2021, p. 31).

Ainda, "é preciso ter em mente que a instituição de boas práticas em proteção de dados não se dá de maneira instantânea. É um processo gradual e que leva tempo e investimento" (Pinheiro; Lotufo, 2021, p. 31).

Neste contexto, para as pessoas jurídicas configurarem-se aos moldes da lei urge uma restruturação na forma de tratamento dos dados pessoais, valendo-se da contratação de estrutura e pessoal especializado, em muitos casos fazendo-se necessário a contratação dos chamados *Data Protection Officers* (DPOs). Esta figura surgiu em decorrência da GDPR e foi espelhada

para a lei brasileira como um funcionário com conhecimentos multidisciplinar, afinal, será necessário que este seja um bom comunicador além de fazer o gerenciamento de crises.

Este cargo - que surgiu com as legislações de proteção de dados, mais precisamente a legislação europeia - é o responsável pela proteção de dados dentro de uma empresa, seja ela pública ou privada, garantindo maior segurança das informações e dados. Este agente precisa conhecer com profundidade os dados aos quais a empresa tem acesso, fazer toda a sua organização, processamento e participar de sua governança (Zilli, 2021).

Além de contratar pessoal especializado, a empresa deve investir em Tecnologia da Informação (TI), em *softwares* e plataformas seguras que privilegiem a transparência e várias outras medidas que corroborem para a adequação do ambiente empresarial às exigências legalmente exigidas. Gastos e mais gastos são necessários para adaptação aos ditames da Lei.

Embora as mudanças demandem gastos e estes sejam significativos, independentemente se a empresa for de pequeno, médio ou grande porte, o risco de incorrer alguma infração trazida pela LGPD e de a empresa ter que arcar com multas e demais sanções será, certamente, mais danoso. Isso porque os gastos com a implementação serão proporcionais ao tamanho da empresa e aos riscos econômicos aos quais seu negócio está inserido.

No entanto, para uma empresa pequena ter que gastar um volume pequeno/médio de dinheiro para ter seus dados mais bem guardados é tão ou mais difícil do que uma empresa de grande porte (que tem melhores condições financeiras), e terá que gastar um volume vultuoso para se adaptar às novas exigências legais. Aqui a relação talvez não seja diretamente proporcional e aí exista um outro problema econômico e de mercado.

Outro aspecto imprescindível para a empresa estar em conformidade com a LGPD e evitar as temerosas sanções é elaborar um contrato claro e objetivo, com finalidade explícita e específica do tratamento de dados para consentimento do titular da informação. Tal contrato entre a empresa e a outra parte (de quem a empresa acessa às informações/dados) deve prever, também, o livre acesso do titular às informações compartilhadas, permitindo que ele exclua, corrija ou torne anônimo seus dados pessoais.

Em relação aos órgãos públicos, uma dificuldade que pode ser apresentada na observância da lei é o que diz respeito ao compartilhamento de dados, uma vez que o compartilhamento faz parte das atribuições da maioria dos órgãos e com a lei é preciso preencher os requisitos exigidos de modo a não sofrer interrupções no tratamento de dados pelo poder judiciário e/ou Autoridade Nacional de Proteção de Dados, além de outras sanções.

Magacho e Trento (2021, p. 16) ressaltam essa situação, em artigo publicado na Revista Brasileira de Pesquisa Jurídica:

> O grande desafio da Administração Pública será em relação ao compartilhamento dos dados pessoais sem comprometer a proteção e segurança das informações, desde a coleta até a sua destruição, visto que a interoperabilidade é permitida, observados os pressupostos do atendimento de políticas públicas ou da prestação de serviços públicos. Nota-se que o compartilhamento de dados pelo Poder Público a entidades privadas é vedado, exceto nos casos de execução descentralizada de atividade pública para finalidade específica e determinada, nos casos em que os dados forem acessíveis publicamente, baseadas em contratos, convênios ou instrumentos congêneres ou na hipótese exclusiva de prevenir fraudes ou proteger a segurança do titular dos dados.

Denota-se que o Poder Público está diante de uma grande dificuldade quando se trata do compartilhamento de informações de dados pessoais, pois não pode comprometer a segurança destas informações, desde o momento que tem acesso a elas, até o momento que a compartilha entre seus servidores – distribuição.

Dessa forma, o Poder Público deve se adaptar as restrições e cuidados com o tratamento de dados pessoais, assim como as empresas privadas, pois mesmo possuindo algumas liberalidades por se tratar de interesse público, os princípios regidos pela lei devem ser respeitados e as motivações bem fundamentadas perante a fiscalização competente.

Com efeito, algumas das críticas em torno da Lei nº 13.709/2018 dizem respeito a complexidade e detalhamento de exigências no que tange as pessoas jurídicas. O dispendioso gasto para sua implantação, principalmente para as médias e pequenas empresas, a ausência de informações mais peculiares e assertivas quanto ao Poder Público, aliado ao medo das infrações penais para quem não se adaptar as exigências legais, são fatores impactam negativamente na execução da lei de proteção de dados pessoais. Entretanto, analisando o ambiente criado pelo avanço tecnológico, ainda que as pessoas jurídicas encontrem algumas dificuldades nas modificações necessárias para se adaptarem a nova realidade, os benefícios que a LGPD traz são inegáveis.

Em primeiro lugar, e bastante óbvio, é a proteção dos dados pessoais dos indivíduos, permitindo uma maior liberdade de expressão, principalmente nos meios digitais, sem o risco dessas informações serem captadas e utilizadas por terceiro de má-fé. Após o incidente com o caso Cambridge Analytica passou-se a ter ciência do quanto os dados circularizados pela Internet são de grande valia e podem influenciar não só a vida das pessoas, individualmente, mas de nações inteiras quando se trata, por exemplo, de eleições ou de fatos econômicos como a venda de grandes corporações.

Estendendo esse benefício para a relação cliente - empresa, a pessoa natural também passa a ter mais segurança jurídica ao permitir o acesso e tratamento de seus dados pessoais, pois tanto seus direitos quanto as responsabilidades da empresa estão bem definidas em lei e sob a ótica da claridade e transparência.

Por segundo, e diretamente relacionado com o primeiro, está a liberdade de decidir como e com quem compartilhar seus dados pessoais a partir do conhecimento da finalidade com que os dados serão tratados, podendo a pessoa natural autorizar o tratamento, bem como retirar seu consentimento. Esta autonomia e ciência quanto a cada etapa do processo de tratamento de dados faz da sociedade mais integrada e mais consciente sobre as informações e sobre o compartilhamento de dados, principalmente os virtuais, evitando situações de manipulações indevidas.

No caso de dados economicamente vendáveis, a ciência quanto a esta monetização, permite ao emissor da informação a legitimidade de consentir ou não com a divulgação de determinada opinião, pensamento, ideia etc. Uma sociedade mais bem preparada no uso de informações tecnológicas, no manejo do direito digital é tão eficaz para o país em suas relações nacionais quanto o torna apto nas suas relações internacionais.

Para melhor entender a relevância da lei em um contexto globalizado, a Doutora em Direito Internacional e Propriedade Intelectual pela USP, PhD, Patrícia Peck Garrido Pinheiro, explica sobre a criação da LGPD no mesmo ano que entrou em vigor a GDPR europeia:

> Isso porque o estado que não possui lei de mesmo nível pode passar a sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da região. Considerando o contexto econômico atual, este é um luxo que a maioria das nações, especialmente os da América-Latina, não podem se dar. Os efeitos da GDPR são principalmente econômicos, sociais e políticos. É apenas uma das muitas regulamentações que vão surgir nesta linha, onde se busca trazer mecanismos de controle para equilibrar as relações dentro de um cenário de negócios digitais sem fronteiras (PINHEIRO, 2021, p. 14).

Com efeito, temos que a legislação sobre a proteção de dados é uma necessidade que todas as nações que estão em um contexto político e econômico de contato mútuo precisam ter, para que assim todas as arestas estejam amparadas e bem delineadas. Com isso, resta evidente a relevância da LGPD para que o Brasil mantenha suas boas práticas internas, assim como boas relações internacionais.

3 CONSIDERAÇÕES FINAIS

A Lei Geral de Proteção de Dados Pessoais indica ser a primeira de outras legislações que despontarão para atender as demandas das relações virtuais que movimentam a economia mundial por meio do acesso aos dados pessoais, utilizados e direcionados nos negócios digitais.

A própria LGPD veio após outros institutos normativos a respeito da internet e suas relações, sendo influenciada de maneira mais direta pela GDPR europeia.

A necessidade da criação da Lei 13.709/2018 vem não somente com intuito de regulamentar o tratamento de dados pessoais no país, embora se restrinja a aplicação territorial brasileira, mas vem para atender as exigências internacionais de que todos os países devam ter uma lei específica para proteção de seus dados.

Embora as empresas se deparem com algumas dificuldades na implantação da lei como gastos elevados com contratação de pessoal especializado, como exemplo o DPO, investimento em plataformas mais seguras etc., outros benefícios como a possibilidade de ter creditado de PIS e de COFINS esses gastos, determinados como insumos e respeitados os requisitos de apuração não cumulativa, aparecem como solução para minimizar os custos.

Da mesma forma, as barreiras encontradas pelo poder público que considera ampla a lei, sem maiores especificações quanto ao compartilhamento de dados no caso em que essa atividade é intrínseca a maioria dos órgãos públicos, como acontece com o Fisco, faz equilíbrio com a segurança do contribuinte que se vê obrigado a compartilhar uma infinidade de informações pessoais e agora possui garantia de que esses dados serão tratados de modo a evitar vazamentos indevidos.

Apesar das críticas, a LGPD é de suma importância tanto para a pessoa natural que tem direito a proteção de seus dados e acesso ao processo de tratamento, quanto para pessoa jurídica que ao se adaptar à lei torna-se capacitada a expandir suas atividades a nível internacional.

Com medo das sanções previstas na lei, as empresas têm buscado todos as formas para se enquadrar as exigências estabelecidas e tão logo isso acontecer, vários benefícios e soluções inteligentes irão surgir para dirimir os inconvenientes com as adaptações.

REFERÊNCIAS

ARAÚJO, M. B. de. **Comércio Eletrônico – Marco Civil da Internet – Direito Digital**. CNC, 2017.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 ago. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/CCivil_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 30 set. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 set. 2022.

BONAVIDES, Paulo. **Do país constitucional ao país neocolonial: a derrubada da Constituição e a recolonização pelo golpe de Estado institucional**. São Paulo: Malheiros, 2001.

GARCIA, L. R.; AGUILERA-FERNANDES, E.; GONÇALVES, R. A. M.; PEREIRA-BARRETO, M. R. **Lei Geral de Proteção de Dados (LGPD):** Guia de implantação. Editora: Blucher, 2020.

G1. Uso da internet no Brasil cresce, e chega a 81% da população, diz pesquisa. **G1 – Economia, Tecnologia.** 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/08/18/uso-da-internet-no-brasil-cresce-e-chega-a-81percent-da-populacao-diz-pesquisa.ghtml. Acesso em: 03 ago. 2022.

MAGACHO, B. T. P.; TRENTO, M. LGPD e compliance na Administração Pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público? **Revista Brasileira de Pesquisas Jurídicas**, [S.l.], v. 2, n. 2, p. 7-26, 2021.

NETTO, T. **Tecnologias de Informação e Comunicação e a Lei Geral de Proteção de Dados**. Instituto de Direito Real. 2022. Disponível em: https://direitoreal.com.br/artigos/tecnologias-de-informacao-e-comunicacao-e-a-lei-geral-de-protecao-de-dados. Acesso em: 31 jul. 2022.

NUNES, S. S. F. Lei geral de proteção de dados pessoais (LGPD). **Direito, Negócios & Sociedade**, v. 1, n. 1, p. 49-60, 2021.

PIMENTEL, J. E. de S. Introdução ao direito digital. **Revista Jurídica da Escola Superior do Ministério Público de São Paulo**, São Paulo, v. 13, n. 1, p. 16-39, 2018.

PINHEIRO, P. P. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. **Revista eletrônica [do] Tribunal Regional do Trabalho da 9ª Região**, Curitiba, v. 10, n. 97, p. 75-87, 2021.

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

REDECKER, Ana Cláudia. et. al. **Proteção de dados: temas controvertidos**. Coordenado por SARLET, Gabrielle Bezerra Sales; TRINDADE, Manoel Gustavo Neubarth; MELGARÉ, Plínio: São Paulo: Editora Foco, 2021.

SLEIMAN, Cristina. et. al. **Segurança digital: proteção de dados nas empresas**. Coordenado por PINHEIRO, Patrícia Peck. São Paulo: Atlas, 2021.

TEFFÉ, C. S. de; MORAES, M. C. B. de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Pensar-Revista de Ciências Jurídicas**, v. 22, n. 1, p. 108-146, 2017.

TOMASEVICIUS FILHO, E. Marco Civil da Internet: uma lei sem conteúdo normativo. **Estudos Avançados**, v. 30, p. 269-285, 2016.

ZILLI, F. **Os desafios para as empresas diante a adequação e regulamentação a Lei 13.709/2018**. 2021. 60 fls. Trabalho de Conclusão de Curso (Bacharel em Direito) – Centro Universitário Curitiba, Faculdade de Direito de Curitiba, 2021. Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/18637. Acesso em: 10 ago. 2022.

Data de submissão: 10/04/2023
Data de aprovação: 30/04/2023
Data de publicação: 28/02/2024