FACULDADE DE DIREITO DE VITÓRIA
CURSO DE GRADUAÇÃO EM DIREITO

JOANNA RIBEIRO VIEIRA

LEI GERAL DE PROTEÇÃO DE DADOS: BENEFÍCIOS E OBSTÁCULOS DIANTE DA ATIVIDADE EMPRESARIAL

VITÓRIA
2021

JOANNA RIBEIRO VIEIRA

LEI GERAL DE PROTEÇÃO DE DADOS: BENEFÍCIOS E OBSTÁCULOS DIANTE DA ATIVIDADE EMPRESARIAL

Monografia apresentada ao curso de Direito da Faculdade de Direito de Vitória – FDV, como requisito para obtenção do título de Bacharel em Direito.
Orientadora: Professora Ma. Ivana Bonesi Lelis

VITÓRIA

2021

LEI GERAL DE PROTEÇÃO DE DADOS: BENEFÍCIOS E OBSTÁCULOS DIANTE DA ATIVIDADE EMPRESARIAL

Monografia apresentada ao Curso de Direito da Faculdade de Direito de Vitória – FDV, como requisito para obtenção do título de Bacharela em Direito.

Aprovada em ___ de dezembro de 2021.

COMISSÃO EXAMINADORA

_____

Prof. Ma Ivana Bonesi Lellis
Faculdade de Direito de Vitória
Orientadora

_____

Prof.

“Aquele que habita sob a proteção do Altíssimo, que moras à sombra do Onipotente, dize ao Senhor “Sois meu refúgio e minha cidadela, meu Deus, em quem eu confio”.

- Salmos 90, 1-2

RESUMO

A Lei nº 13.709, de 14 de agosto de 2018 dispõe acerca do tratamento de dados pessoais no Brasil. Com forte inspiração na GDPR (Regulamento Geral de Proteção de Dados) europeia, a Lei Geral de Proteção de Dados (LGPD) trouxe diretrizes para a coleta e tratamento dos dados pessoais manuseados pelas instituições. Diante disso, a norma insere o Brasil no cenário mundial de busca por melhores práticas de governança de dados. A implantação do novo Regulamento objetiva a proteção ao direito de privacidade e intimidade do indivíduo diante da maior segurança e transparência em relação à manipulação e compartilhamento das informações pessoais. O objetivo do presente trabalho é analisar a aplicabilidade da Lei Geral de Proteção de Dados nas empresas brasileiras. Ao longo do estudo, conclui-se que a aplicação da LGPD é indispensável para o bom funcionamento das instituições no atual contexto tecnológico mundial. Salienta-se aqui, a importância da lei para a atividade empresarial, de forma que esclarece e regulamenta a coleta, o tratamento, o armazenamento e o compartilhamento dos dados, assegurando aos indivíduos maior segurança e proteção no tratamento de seus dados.

Palavras-chaves: Lei Geral de Proteção de Dados. LGPD. Dados Pessoais. Privacidade. Adequação da Atividade Empresarial. Custos e Riscos.

SUMÁRIO

INTRODUÇÃO

A partir de 14 de agosto de 2018, o Brasil passou a integrar o grupo de países que promovem uma abordagem jurídica específica acerca da Proteção de Dados. Nessa perspectiva, apesar de já possuir dispositivos legais vagos acerca do tema, com a sansão da Lei nº 13.709, a legislação brasileira passa a dispor de uma tutela mais específica e particular do assunto.

Salienta-se que o Direito necessitou se adaptar às mudanças advindas do novo contexto tecnológico. Isto é, as inovações digitais se desenvolvem de maneira desmedida, em moldes jamais testemunhados. Assim, as informações passaram a ser disseminadas facilmente, e, portanto, geradas e propagadas em larga escala. Diante disso, a tutela jurídica atua de maneira a se ajustar às novas formas de relações sociais e jurídicas.

Destarte, demonstrou-se necessária a imposição de limites morais à coleta, manipulação e compartilhamento dos dados pessoais. Bem como, a revolução tecnológica acarretou em uma demanda por proteção de bens incorpóreos, como a informação.

Nas últimas décadas, a coleta de dados passou a ocorrer sucessivamente, de modo online ou off-line. Nesse sentido, os bancos de dados vivenciam uma enorme expansão de sua capacidade de processamento e armazenamento de informações, tanto de consumidores e usuários como dos fornecedores. Nessa conjuntura, surge um maior cuidado com a intimidade dos indivíduos que tem seus dados manuseados.

O presente estudo irá explicar o conceito de base de dados, suas classificações, como se dá o tratamento de dados e quais os são os sujeitos de direito afetados por essas novas relações. Será ponderado, ainda, como a nova Lei afetará o setor privado, em razão das adaptações e cautelas que impõe. Quais são os impactos positivos e negativos da LGPD na atividade empresarial, bem como, seus custos, sansões e riscos diante do novo contexto brasileiro.

1 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

1.1 APLICAÇÃO E PRINCÍPIOS DA LGPD

Por força dos modernos meios de coleta de dados dos indivíduos, surgiu a necessidade da criação de uma lei que garantisse a proteção da intimidade e inviolabilidade da vida privada. Diante dessa preocupação, foi sancionada em 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (13.709/2018), com o objetivo de regulamentar a prática do tratamento de dados, a fim de proteger os direitos fundamentais de liberdade e de privacidade.

Conforme conceitua Rafael Fernandez Maciel na sua obra “Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais”:

> A LGPD é uma lei que dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade natural, inclusive por meio digital. (MACIEL, 2020, p. 79)

A Lei traça uma uniformização do manual de como deverá ser realizado o tratamento dos dados, definindo os direitos e deveres, criando um perfil ético, por meio do esforço mundial para que se tenha maior segurança sobre as informações e privacidade de dados. Assim, o seu objetivo é permitir que o cidadão tenha mais controle sobre o tratamento de suas informações pessoais. (CANDIDO, ARAÚJO, RIBEIRO, 2021).

O ordenamento surgiu com o intuito de proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Diante disso, a LGPD dispõe sobre o tratamento de dados feito por pessoa física ou jurídica de direito público ou privado englobando um amplo conjunto de operações efetuadas em meios manuais ou digitais. (LGPD, 2021)

A nova legislação se aplica às organizações que gerenciem bases de dados com fins econômicos; dados tratados dentro do território nacional, independentemente do meio aplicado; e dados usados para fornecimento de bens ou serviços.

Dessa forma, a lei aborda, em seu artigo 6°, os princípios que devem ser seguidos ao realizar tratamentos de dados pessoais.

> O inciso I trata do princípio da finalidade, o qual prima pela realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. Adiante, o inciso II trata do princípio da adequação, o qual se refere à compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. (PESTANA, 2020)

Ainda, o princípio da necessidade se consubstancia na limitação da realização do tratamento ao mínimo necessário para a execução do seu propósito, abarcando os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. Ou seja, somente deverão ser tratados os dados pertinentes, ou seja, aqueles que se mostrem imprescindíveis para que o objetivo previamente tracejado seja atingido. (PESTANA, 2020)

Cabe salientar, também, que um dos princípios cardeais da LGPD no tocante ao tratamento é princípio do livre acesso. Este estabelece que os titulares dos dados possam consultar de modo gratuito e fácil a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais. Ainda, o inciso V do referido artigo dispõe sobre a qualidade dos dados. Este princípio se pauta na garantia, assegurada aos titulares dos dados, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. (PESTANA, 2020)

Ademais, o princípio da transparência, disposto no inciso VI do art. 6º da LGPD estabelece que aos titulares dos dados deve ser garantido e assegurado informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e sobre os respectivos agentes de tratamento, resguardados os segredos industriais e comerciais. Ainda, o princípio da segurança e da prevenção, respectivamente dispostos nos incisos VII e VIII, incentivam a preservação, sempre

em ambiente seguro, dos dados das pessoas naturais objeto do tratamento. Para tanto deverão ser utilizadas, sempre, medidas técnicas e administrativas de segurança. (MATOS, 2021)

Por fim, a LGPD assentou, expressamente, o impedimento de realização do tratamento de dados a fim de cometer discriminação ou abuso por meio do princípio da não discriminação. Diante disso, em seu último inciso impôs a necessidade de demonstração, pelo agente, da adoção de medidas competentes a fim de comprovar a efetividade das normas de proteção de dados pessoais.

Isto posto, conclui-se que a aplicação de tais princípios representa uma tendência rumo à constatação da autonomia da proteção de dados pessoais e à sua consideração como um direito fundamental. No cenário internacional, observa-se que os países que sofreram mudanças de regime político, foram os primeiros a promover a reelaboração de suas Constituições elevando a problemática relacionada à informática e à informação pessoal em nível constitucional. (DONEDA, 2011, p. 101)

Ante todo o exposto, considerando que o tratamento de dados diz respeito a uma intromissão da vida pessoal do titular, é fundamental que sejam seguidos princípios determinados em lei, e que o titular tenha total liberdade para aceitar ou recusar tal tratamento, bem como ter ciência de quais dados serão processados e com qual finalidade.

1.2 LGPD E O CONTEXTO MUNDIAL

No que se refere ao contexto mundial, em 2012, surge na União Europeia, o RGPD (Regulamento Geral de Proteção de Dados). Essa lei, que entrou em vigor em 2018, passou a regular todo o tratamento de dados dos países pertencentes à União Europeia, influenciando, inclusive ao Brasil, a criar seu próprio regulamento.

Aprovada pelo Regulamento (EU) 2016/679 do Parlamento Europeu e o Conselho, em 27 de abril de 2016, a RGPD se tornou o ponto de referência em relação a forma de tratar os dados pessoais. (BEZERRA, 2020)

Segundo Pinheiro (2020, p. 6), a aprovação da RGPD, ocasionou a obrigação para os demais países, exigindo o desenvolvimento de regulamentações do mesmo nível que tratassem da proteção de dados pessoais, para, assim, evitar empecilhos ou dificuldades de negociações com países da União Europeia, caso optassem por manter ligações comerciais com à mesma.

Ademais, em 2013, Edward Snowden, ex-técnico da CIA, divulgou diversos esquemas de espionagem por parte dos EUA, relatando um uso mal intencionado de dados pessoais. Tal caso teve uma enorme repercussão e, no âmbito brasileiro, acelerou a criação do Marco Civil da Internet, conjunto de leis que busca regular o uso da internet, apesar de não tratar tanto sobre dados pessoais quanto a sua sucessora, a LGPD. (CANDIDO, ARAÚJO, RIBEIRO, 2021).

Mais à frente, em 2018, ocorreu o escândalo da empresa Cambridge Analytica[1], o qual revelou como os dados recolhidos por meio do Facebook eram utilizados inapropriadamente. Tais dados influenciaram desde as campanhas eleitorais estadunidenses de 2016, até a saída do Reino Unido da União Europeia. (ENTENDA, 2021)

Assim, aumentou-se o alerta internacional para a questão do tratamento de dados. Em razão disso, muitas empresas brasileiras precisaram se adequar a esta nova realidade, resultando no aumento da pressão para a aprovação da LGPD.

[1] Cambridge Analytica (UK), foi uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para o processo eleitoral. Foi criada em 2013, como um desdobramento de sua controladora britânica, a SCL Group para participar da política estadunidense.

1.3 GARANTIAS E DIREITOS

Dentre os mitos compartilhados pelo positivismo jurídico, os mais aceitos e consolidados são os dogmas da coerência, da completude e da unidade do ordenamento jurídico, vetores para a consolidação dos propósitos da segurança e certeza jurídicas exigidos pela sociedade de mercado. (MOREIRA, 2008, p. 173)

Diante disso, o artigo 2º da Lei 13.709/2018 (BRASIL, 2018), dispõe que a proteção de dados tem como fundamentos:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Nesse sentido, Bruno Miragem (2019, p. 02) entende que a proteção de dados pessoais é projeção de direitos fundamentais consagrados. De forma que, associa-se à proteção da vida privada e da intimidade (art. 5º, X, da CF), e da dignidade da pessoa humana (art. 1º, III, da CF).

Ademais, a Constituição Federal de 1988, da mesma forma, garante a inviolabilidade do sigilo de dados (art. 5º, XII) como direito fundamental. Por esse motivo, a proteção de dados pessoais se baseia, “como direito da personalidade, ou a especialização da proteção constitucional à vida privada e à intimidade dando origem a um direito fundamental à proteção de dados pessoais”. (BIONI, 2019)

Diante disso, a restrição do uso de dados pessoais determinada pela nova legislação preconiza o princípio da dignidade da pessoa humana, principalmente, a proteção do direito à liberdade, à privacidade, à honra e à imagem pertencentes ao ser humano. Desse modo, é dever do setor privado fornecer essa segurança aos dados dos consumidores. (NASCIMENTO, 2019)

Dessa forma, é gerada uma expectativa ao titular dos dados, a partir do consentimento, considerando que o fornecedor ou o controlador das informações pessoais não darão utilidade diversa a elas, se não aquelas acordadas previamente, tal qual foi compreendida pelo consumidor. (MIRAGEM, 2019, p. 5)

No campo das relações entre particulares, a autonomia retrata um aspecto ativo e positivo da personalidade, no âmbito de atuação das pessoas que podem atuar como seres autônomos e responsáveis. Assim, na tentativa de relacionar a autonomia com os deveres, no que diz respeito à horizontalidade dos deveres fundamentais, pode-se identificar no constitucionalismo uma ideia simples, a saber: quem possui direitos deve também possuir deveres (DIMOULIS; MARTINS, 2011, p. 339). Tal contraprestação dá-se no caso do indivíduo que tem a sua intimidade preservada, nas redes sociais, por exemplo, e igualmente respeita a intimidade de outrem no mesmo universo virtual. (DUQUE; PEDRA, 2013, p. 153)

Assim, a necessidade de aplicação dos deveres fundamentais aos particulares em suas relações (horizontalidade dos deveres fundamentais), sobretudo pautando-se na solidariedade, não pode descuidar do respeito à autonomia privada a partir de fundamentos mais básicos da economia. (DUQUE; PEDRA, 2013, p. 154)

Como adverte Adriano Sant'Ana Pedra (2010, p. 10), “a natureza dinâmica da Constituição como organismo vivo que é, permite que ela possa acompanhar a evolução das circunstâncias sociais”. Assim sendo, a instituição ou não de deveres fundamentais repousa na soberania do Estado enquanto comunidade organizada.

Zanon (2013, p.160) ainda afirma, que o direito à proteção dos dados pessoais, como direito fundamental, possui duas dimensões: uma subjetiva (status negativo) sendo um direito de resistência, ao delimitar uma esfera de proteção que não pode sofrer intervenção indevida do poder estatal ou privado, exigindo a abstenção do Estado nesse âmbito e, também, uma dimensão objetiva (status positivo), na medida em que reclama ações do Estado para garantir tal proteção.

Neste sentido, pode-se afirmar que a proteção de dados pessoais garantida pela LGPD é um direito fundamental de status positivo, ou seja, é uma proteção prestada

pelo Estado, pois é quem tem o dever de criar políticas e estabelecer normas que devem ser seguidas pelo setor privado. (NASCIMENTO, 2019)

Fundamenta-se a LGPD no propósito de garantia dos direitos do cidadão, oferecendo bases para o desenvolvimento econômico a partir da definição de marcos para utilização econômica da informação decorrente dos dados pessoais. (MENDES, DONEDA, 2018, p. 471)

1.4 DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS

A Comissão Europeia define dados pessoais como:

> informações relativas a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. Dados pessoais que tenham sido descaracterizados, codificados ou pseudonimizados, mas que possam ser utilizados para reidentificar uma pessoa, continuam a ser dados pessoais e são abrangidos pelo âmbito de aplicação do RGPD. Dados pessoais que tenham sido tornados anónimos de modo a que a pessoa não seja ou deixe de ser identificável deixam de ser considerados dados pessoais. Para que os dados sejam verdadeiramente anonimizados, a anonimização tem de ser irreversível. (UNIÃO EUROPEIA, 2018)

Espelhando-se no RGPD da UE, a Lei 13.709/2018, também faz uma separação entre dados pessoais e dados pessoais sensíveis:

> Art. 5º. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018)

Pela LGPD existem três tipos de dados: os dados pessoais, os dados pessoais sensíveis e dados anônimos. Sendo considerado como dados pessoais toda e qualquer informação que possa ser vinculada a uma pessoa identificada ou identificável. Dados pessoais sensíveis são qualquer dado que pode levar a algum tipo de discriminação, por exemplo, religião, vida sexual, dado genético. Por fim,

dado anônimo é aquele que deixa de ser diretamente relacionado a uma pessoa, ou seja, quando um conjunto de dados se torna estatística.

Dessa forma, há uma atenuação ao princípio da privacidade ao tratar os dados pessoais sensíveis. Deverá haver uma cautela ainda maior, justamente por serem dados que são ainda mais íntimos e privados do titular. Diante disso, o legislador foi cuidadoso ao separar as hipóteses de tratamento dos dados sensíveis dos demais, no art. 11º da Lei:

> **Art. 11**. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (BRASIL, 2018)

Observa-se que a lei trouxe consigo uma certa limitação de aplicabilidade em relação aos tipos de dados que são regulados pela LGPD. “O tratamento de dados pessoais deve seguir um propósito certo e funcional, mas que não supere a liberdade de informação e expressão, a soberania, segurança e a defesa do Estado” (PECK, 2018, p. 43-44).

São exemplos de dados pessoais o nome ou apelido, o endereço de uma residência ou de correio eletrônico, o número de um cartão de identificação, dados de localização, um endereço IP, o número do seu telefone e até mesmo os dados detidos por um hospital ou médico, que permitam identificar uma pessoa de forma inequívoca. (SILVA, 2021)

Tal sociedade da informação compreende o uso de redes sociais, como o Facebook, Instagram e Twitter, assim como aplicativos, como o Whatsapp e Tinder, e lojas de compras online como OLX e Mercado Livre. Porém, em um contexto mais amplo, envolve também os cadastros de consumidores em lojas e hospitais, os dados sobre processos judiciais, débitos fiscais, assim como bancos de dados privados de empregadores e públicos da administração do governo. É difícil imaginar qualquer aspecto da sociedade atual que não esteja ancorado numa plataforma digital, que contém praticamente todas as informações constitutivas das relações sociais, econômicas e jurídicas em geral. (PINHEIRO; BONNA, 2020, p. 368)

Para Ribeiro (2016), os dados pessoais são cumulações de fatos e acontecimentos que formam a personalidade de cada indivíduo, de maneira que podem contar de forma precisa a história de vida de cada cidadão.

A informação pessoal, aqui tratada, deve observar certos requisitos para sua caracterização. Determinada informação pode possuir um vínculo objetivo com uma pessoa, revelando algo sobre ela. Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras. (DONEDA, 2011, p. 93)

Diante disso, cabe elencar no presente estudo alguns conceitos acerca do tema. A base de dados é um conjunto de informações referentes a um determinado setor do conhecimento humano, está organizada por meio de programas de computador especialmente desenvolvidos para esta finalidade, e é suscetível de ser utilizada em várias aplicações. (WACHOWICZ, 2005, p.13)

Ainda, entende-se por titular, o indivíduo dono dos dados pessoais que serão tratados. Este deve autorizar ou não o tratamento dos dados. Já agentes de tratamentos são os controladores e operadores. Controlador é o responsável pelas decisões relacionadas ao tratamento dos dados pessoais, bem como por qualquer

incidente que venha a ocorrer. Já operador é aquele quem trata os dados e deve seguir todas as ordens do controlador em relação ao tratamento dos dados.

Por fim, a Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por implementar e gerenciar as regras da LGPD, diante da realização de auditorias, bem como pela aplicação das devidas sanções em descumprimento da Lei.

1.5 PRIVACIDADE

As barreiras entre a vida privada e a vida pública se ruíram diante do avanço tecnológico presenciado em todo mundo. À vista disso, a privacidade do indivíduo passou a ser analisada sob um novo olhar, demandando mais atenção e segurança, considerando a fácil acessibilidade e compartilhamento dos dados pessoais.

Conforme explica RODOTÁ (2008, p. 92), a privacidade na era da informação deverá ser definida pelo direito do sujeito de manter o controle sobre as próprias informações. Nesse sentido, valorizam-se as escolhas pessoais, levando em conta o novo poder que o indivíduo possui sobre o tratamento de seus dados.

Isto posto, com a chegada dos Regulamentos de Dados, o indivíduo passou a ter um poder de controle sobre suas informações. Entretanto, viu-se a chegada de sérias ameaças cibernéticas, impondo ao Direito o dever de agir para tutelar a privacidade do sujeito. (PANEK, 2019, p. 15)

Assim, torna-se fundamental para a defesa dos direitos fundamentais do titular, a tutela dos seus dados. Isso porque, o usuário do ciberespaço configura uma nova forma de vulnerabilidade, uma vez que tramita livremente em um meio extremamente volátil e veloz, exposto a riscos inerentes à natureza impessoal e incorpórea do meio digital. Da mesma forma como exposto que o conceito da privacidade deve absorver nova interpretação, as definições de consumidor e da boa-fé também precisam de um novo filtro diante da era informática. (PANEK, 2019, p. 16)

Outro ponto marcante da sociedade da informação que tenciona a privacidade é que, quanto mais o setor público e o setor privado se tornam dependentes das tecnologias da informação, mais sujeitos estarão a ataques de pessoas mal-intencionadas. Nesse afã de supervalorizar a tecnologia da informação, “quanto mais um governo e uma sociedade dependem de sua rede de comunicação, maior sua exposição a ataques de hackers, crackers e de organizações criminosas, crescendo crimes cometidos em meio eletrônico” (VIEIRA, 2007, p. 162-163)

Para fins da LGPD, considera-se consumidor o titular dos dados pessoais. O consumidor no CDC, tem um conceito amplo materialmente, atingindo atos ilícitos pré-contratuais e defendendo a coletividade perante acidentes de consumo, ainda que não tenham utilizado do produto ou serviço como destinatários finais. (MARQUES, 2014, p. 98).

O direito a proteção de dados está relacionado a um direito de personalidade, não de propriedade. Isso porque a propriedade está diretamente relacionada à fins econômicos, enquanto, os dados pessoais sensíveis não estão, ou pelo menos não deveriam estar relacionados à fins negociais. Dentro da cultura mercadológica de processamento de dados, as informações pessoais dos indivíduos deixam de ser elementos sensíveis advindos de uma individualidade, e passam a se algoritmos, tratados por uma cadeia de processos até chegarem a quaisquer que sejam os objetivos das empresas. RODOTÁ (2008, p. 19)

Portanto, em virtude da nova era digital, se faz necessário ao Direito oferecer meios de proteção e controle de dados ao cidadão, bem como estipular limites morais aos controladores de informação, tanto no setor privado como no setor público, em favor do direito à intimidade.

1.6 TRATAMENTO DE DADOS

A disseminação do uso de computadores fez com que, nos dias atuais, não somente as agências governamentais que tradicionalmente coletavam dados pessoais, a

exemplo dos Correios, os Departamentos de Trânsito e as repartições do Fisco, funcionassem como poderosos centros de processamento de informações pessoais, mas também todas as empresas privadas hoje adquiriram os meios para coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo. (REINALDO, 2002, p.26)

A Lei Geral de Proteção de Dados entende o tratamento de dados como:

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (BRASIL, 2018)

Assim, a LGPD se aplica a todo e qualquer tratamento de dados, realizado por pessoa física ou jurídica, voltado para fins comerciais, desde que o tratamento seja realizado todo ou em parte no território nacional. A Lei não será aplicada em tratamentos de dados com fins não econômicos, ou que seja realizado para fins jornalístico e artísticos, em casos de segurança pública e do estado e defesa nacional, e de dados de fora do país e que não seja compartilhado com agentes brasileiros.

Ainda, a Lei engloba outros conceitos para que haja ou não o tratamento de dados:

> Consentimento: permissão dada pelo titular para que determinado(s) dado(s) pessoal(is) seja(m) tratado(s). Deve ser pedido de forma explícita, clara e transparente pelo operador ou controlador, e se referir a uso específico e limitado. Bloqueio: suspensão do tratamento de dados, que não isenta o operador e o controlador de precisarem proteger os dados pessoais e o banco de dados em que eles se encontram. Eliminação: exclusão de dados pessoais. (GONZALES, 2019)

Segundo Ribeiro (2016, p.4), o consentimento para o tratamento de dados é parte importante para que haja o respeito ao direito à liberdade de escolha, e deve ser livre, informada, inequívoca, específica, determinada e expressa.

O consentimento é a principal ferramenta para que haja o tratamento de dados, e deve ser respeitada a forma prevista em lei, seja por escrito ou qualquer meio que

demonstre a vontade do titular, podendo ser revogado a qualquer momento. (DONEDA, 2020, p. 35)

Insta salientar que o consentimento não é sempre obrigatório. Em casos que o tratamento visar o cumprimento de leis e de políticas públicas, para órgãos de pesquisa, na execução de contratos ou para o exercício regular de direitos, e também em casos de tutela da saúde e proteção da vida não é necessário o consentimento.

Não se tratando das exceções que dispensam o consentimento do titular, o controlador mesmo que já esteja de posse dos dados, se precisar tratá-los com outra finalidade, deve pedir novamente o consentimento do titular.

1.7 SEGURANÇA DOS DADOS PESSOAIS

A segurança pode ser entendida como um conjunto de medidas que visam à proteção de riscos, perigos ou perdas a pessoas ou coisas. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." (BLUEPHOENIX, 2008).

Conforme expõe Mário Antunes (2019), “as perdas não são apenas monetárias, já que há custos que poderão ser de difícil contabilização, como a perda de credibilidade ou a publicidade negativa”.

Os dados pessoais e dados sensíveis tem um valor exponencial, e caso esses dados sejam roubados ou perdidos, as empresas podem pagar um preço muito alto para recuperá-los ou para sanar os efeitos dos danos causados. Além da multa em dinheiro, pode perder a confiança dos seus clientes, investidores e parceiros.

Ante o exposto, tratando-se de um assunto relativamente recente, nem todos os indivíduos estão familiarizados e cientes do quão valiosos os seus dados pessoais

são para o mercado, e nem como os mesmos são coletados, armazenados e compartilhados, de forma que uma simples falha de segurança os deixe expostos.

Segundo Sérgio Ricardo Correia (2018, p.8):

> Diariamente, algoritmos são alimentados por informações pessoais que indicam como pensamos e quais os nossos desejos, criando perfis de consumo dos usuários, para fins de publicidade direcionada e venda desses dados pessoais para outras empresas. Nesse sentido, a proteção da privacidade passa pela proliferação dessas práticas comerciais de “big data”, “targeting” e “profiling” dos usuários, deixando as pessoas presas dentro de uma realidade on-line customizada (“tailored reality”).

Tornou-se frequente, ao efetuar uma compra na internet ou fisicamente, a situação de ser obrigado a preencher cadastros com diversas informações pessoais. Hoje em dia, com os programas de educação fiscal, informar o CPF no momento de uma compra é imprescindível, mas nem todos os dados solicitados são necessários. Ocorre que, esses dados ficam registrados, seja para criar um perfil do usuário, a fim de oferecer conteúdo publicitário direcionado, ou para vendê-los a outras empresas.

De acordo com Ricardo (2018, p.9), a vida de uma sociedade hiper conectada é decidida por algoritmos automatizadas, e vários dos tratamentos desses algoritmos são feitos por inteligências artificiais. No entanto, com a LGPD, é possível solicitar a exclusão desses dados após o término da relação comercial entre as partes.

O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. (DONEDA, 2011, p. 92)

O direito à eliminação de dados está disposto no art.18° da LGPD, onde estabelece que o titular pode solicitar ao controlador, a qualquer momento e mediante requisição:

> **Art. 18**. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
> I - confirmação da existência de tratamento;
> II - acesso aos dados;
> III - correção de dados incompletos, inexatos ou desatualizados;
> IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - 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;
> VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
> VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
> VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
> IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (BRASIL, 2018)

Diante disso, é fundamental que as organizações que tratam os dados pessoais observem o disposto na LGPD, agindo de acordo com as normas. É de extrema importância a implantação dos procedimentos necessários para garantir a segurança dos dados, afim de evitar as penalidades previstas.

2 IMPOSIÇÕES DA LGPD ÀS EMPRESAS

2.1 OS DADOS COMUMENTE TRATADOS EM EMPRESAS

A chegada da LGPD, introduzindo novas obrigações, práticas e rotinas às empresas, agora chamadas de controladores, somada às consequências administrativas do seu eventual descumprimento, força a necessidade de um novo olhar sobre a natureza dos dados pessoais e sobre a forma como tais informações devem ser tratadas, dentro do ambiente empresarial.

Isto posto, a Lei traça normas objetivas e cristalinas acerca do manuseio, coleta, armazenamento e compartilhamento dos dados pessoais de usuários, seja em meios digitais ou físicos. Diante disso, toda organização se vê na obrigação de corresponder e seguir a legislação atual, sujeitando-se às penalidades impostas.

Cabe ressaltar que, um empreendimento processa distintos dados, seja de seus consumidores, funcionários ou fornecedores. Dados estes como nome, endereço, e-mail, RG, Cadastro de Pessoa Física (CPF), preferências, gostos e todas essas informações estão taxadas como dados pessoais pela LGPD. Ou seja, são dados protegidos por lei, e devem ser solicitados, além de informados ao titular de forma clara sobre como serão tratados, qual a finalidade ou se serão compartilhados.

2.2 A IMPLANTAÇÃO DA LGPD NAS EMPRESAS

Considerando o rol de inovações trazido pela LGPD, torna-se necessária a adoção de medidas de implementação de mecanismos internos e sistemas de controle para garantir a conformidade com a legislação, a fim de proteger os dados pessoais de quaisquer riscos de incidentes que possam ocorrer.

Dessa maneira, a instituição deve provar que está de acordo com a Lei, bem como que possui o consentimento do titular dos dados. Para isto, é necessário atender a

todos os princípios estabelecidos pela LGPD, antes de processar e fazer uso dos dados alheios. Revela-se fundamental, ainda, demonstrar que a organização possui infraestrutura suficiente para preservar tais dados. Para viabilizar tal tarefa, as empresas podem guiar-se pelos parâmetros estabelecidos pela ISO 27001[2].

De acordo com o site Advisera (2020):

> A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela é escrita pelos melhores especialistas mundiais no campo de segurança da informação e provê metodologia para a implementação da gestão da segurança da informação em uma organização. Ela também possibilita que organizações obtenham certificação, o que significa que um organismo certificador independente confirmou que uma organização implementou a segurança da informação em conformidade com a ISO 27001.

Nesse contexto, trata-se de uma árdua tarefa para a empresa adequar-se a todas as normas impostas. É necessário a realização de análises de riscos e adoção de medidas preventivas, com o intuito de adequar a execução das atividades da organização às normas.

Marcelo Tostes (2020) entende que, uma equipe de TI capacitada pode contribuir muito com a segurança de dados da empresa, podendo evitar grandes riscos através da elaboração de uma política interna de uso de recursos digitais. Além de adotar todas as medidas possíveis, é importante elaborar relatórios de riscos, evidenciando as fragilidades, os riscos a que cada setor da empresa está exposto, bem como os incidentes ocorridos e como foram resolvidos, fazendo com que as políticas internas sejam direcionadas e tenham maior eficácia.

Natália Chaves e Lucas Guimarães (2020) afirmam que, a fim de se evitar infringência às disposições legais e, consequentemente, reduzir o risco de aplicação de sanções, devem ser promovidas, por parte dos empresários, as adequações às exigências estabelecidas pela LGPD, dentre as quais destacam-se:

---

[2] Disponível em: https://www.iso.org/isoiec-27001-information-security.html. Esta norma foi elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). A adoção de um **SGSI** deve ser uma decisão estratégica para uma organização.

> (i) nomeação de um encarregado; (ii) definição dos agentes de tratamento, a saber, controlador (quem toma as decisões sobre o tratamento de dados) e operador (quem realiza o tratamento); (iii) revisão das políticas de segurança, com a adoção de medidas aptas à proteção dos dados pessoais; (iv) manutenção de registros das operações de tratamento de dados pessoais; (v) formulação de regras de boas práticas e implementação de governança em privacidade de dados; (vi) revisão de contratos e de demais instrumentos formalizados com terceiros e fornecedores em geral que, direta ou indiretamente, recebam ou realizem algum tipo de tratamento de dados, estabelecendo-se, assim, os limites no emprego dessa informação, de modo a adequar o procedimento à LGPD; (vii) elaboração de relatório de impacto de privacidade, como uma forma, inclusive, de fiscalização do cumprimento das disposições legais e de implantação de um efetivo programa de compliance. (CHAVES, GUIMARÃES, 2020)

Ante o exposto, verifica-se que a adaptação das empresas à LGPD acarretará em novos custos e trâmites internos à instituição que está em processo de ajuste. Diante disso, será analisado a seguir os impactos dessas mudanças no cenário empresarial brasileiro.

2.3 IMPACTOS SOBRE A ATIVIDADE EMPRESARIAL

Destarte, as Instituições mais atingidas pela vigência da Lei aqui tratada, são aquelas que detém e processam, em grande escala, diferentes dados do consumidor. Sendo estes os profissionais de marketing, as empresas de tecnologia, bem como coletores de dados que as conectam.

Assim, diante de todos os impactos oriundos da entrada em vigor da LGPD, a abrangência da Lei causa certa apreensão no setor empresarial. Isto porque, a Lei propõe um conceito amplo do que se define como dado e suas espécies. Dessa forma, ante a amplitude do conceito legal, ou seja, qual informação identifica ou torna o indivíduo identificável, as empresas deverão se adequar ao texto normativo rigorosamente no que diz respeito ao tratamento de tais dados coletados no território brasileiro.

Por óbvio que tal adaptação implica um aumento nos custos inerentes ao exercício da atividade econômica. Contudo, tais custos são mínimos se comparados às penalidades decorrentes de eventual descumprimento das exigências legais. Enfatiza-se, ainda, que a LGPD prevê a responsabilidade solidária durante o

processo de tratamento de dados, de modo que a implementação de procedimentos de segurança deve ser observada por todos os envolvidos. (CHAVES, GUIMARÃES, 2020)

Entretanto, a Lei 13.853/2018 traz uma série de inovações e vantagens à atividade empresarial. Isto é, com o novo ordenamento em vigor, passa-se a obter uma garantia legal superior em relação aos atos praticados pela empresa, vez que a nova regulamentação prevê unificar todas as regras relacionadas à privacidade. Ademais, houve uma certa equiparação legal do mercado brasileiro com os demais existentes no contexto mundial, haja vista que muitos países já estão familiarizados com as normas referentes à proteção de dados.

Ainda, ao proporcionar uma relação mais transparente e confiável com o cliente, a devida aplicação da Lei pode promover uma fidelização do cliente, afunilando o público-alvo da organização. De forma que, estabelecendo previamente a finalidade para a obtenção e utilização dos dados, haverá maior confiança e credibilidade no negócio, pois a nova maneira de lidar com os dados passa a ser segura para todos. Dessa forma, a privacidade dos dados, a forma e o fluxo das operações se tornam uma segurança no mercado.

Diante disso, no atual contexto de ameaças constantes e hipóteses crescentes de vazamento de dados de sistemas, a proteção cibernética irá aumentar, considerando que o uso não consentido da plataforma coletora já resulta na violação de informações e determina um alto investimento em gestão de risco e fraude.

Outrossim, a melhora do gerenciamento dos dados coletados e armazenados possibilita um aumento de lucros, haja vista o aprimoramento dos processos atualmente utilizados. Diante disso, é possível analisar que o impacto ocorrerá especialmente na área de marketing de consumo e produtos, tendo em vista que a eliminação de informações irrelevantes e defasadas dos bancos de dados, os tornará mais organizados e eficientes, a nível de informação do consumidor, o que poderá ser revertido no uso de eventuais pesquisas de mercado e consumo direcionadas. (ANDRADE, STEPENOSKI, 2019)

Ademais, a necessidade de anuência para recebimento de campanhas resultará em um potencial consumidor mais qualificado, ou seja, somente os clientes em potencial mais envolvidos permanecerão no banco de dados, proporcionando o direcionamento eficaz do produto diretamente a estes (ANDRADE, STEPENOSKI, 2019).

3 ADAPTAÇÕES DA ATIVIDADE EMPRESARIAL À LGPD

3.1 NECESSIDADE DE ADEQUAÇÃO

A RGPD (Regulamento Geral de Proteção de Dados) é referência mundial no tratamento de dados pessoais. Sua implementação na União Europeia acarretou mudanças diversas tanto para os titulares dos dados, como para as empresas que os manuseiam. Diante desse marco mundial no tratamento de dados pessoais, outros países passaram a rever a forma que regulam o uso dessas informações sensíveis.

O Regulamento entrou em vigor no dia 25 de maio de 2018 e substitui a Diretiva 95/46/EC, formulada nos anos 90. A nova legislação surgiu com o intuito de proteger os dados dos indivíduos frente a nova era tecnológica assegurando a livre circulação desses dados, e, ao mesmo tempo, a transparência por parte dos responsáveis pelo tratamento de dados pessoais e controle das pessoas que se encontram na União Europeia sobre a suas informações. (SILVA, BRANCHER, TALIBERTI, CUNHA, 2018)

Um dos principais aprendizados deixados pela experiência europeia sustenta-se no quão importante é a delimitação do momento da coleta de dados, da consulta ou da contratação, a fim de apurar a real relevância do fornecimento daqueles dados específicos para o propósito negocial pretendido. (ANDRADE, STEPENOSKI, 2019)

Diante disso, a principal diferença entre o Regulamento europeu e o brasileiro consiste no fato de a proteção dos dados pessoais ser considerada um direito fundamental na União Europeia. Diante disso, vejamos:

> Diferentemente da Diretiva - que estabelecia diretrizes para que cada Estado-Membro da União Europeia adotasse sua própria lei de proteção de dados -, o GDPR foi desenvolvido visando à harmonização das leis de proteção de dados dos países da União Europeia, sendo vinculativo e aplicável a todos os Estados-Membros. Por outro lado, o GDPR também garante aos Estados-Membros certa margem de autonomia para elaborarem disposições mais específicas para adaptar a aplicação das

> regras previstas no Regulamento. (SILVA, BRANCHER, TALIBERTI, CUNHA, 2018)

Vê-se que a proteção à intimidade e à vida privada é um valor democrático essencial que precisa ser concretizado. Com o avanço e o surgimento de novas tecnologias, é preciso regulamentar e controlar a utilização dos dados pessoais para salvaguardar os direitos fundamentais, tendo em vista que possuem conteúdo econômico e podem ser comercializados (LIMBERGER, 2008, p. 218).

Diante disso, para cumprir com as exigências previstas, as empresas terão um procedimento trabalhoso para adequação, uma vez que será preciso desenvolver medidas, regras e políticas. É de suma importância designar a responsabilidade a um grupo de profissionais para realizar um levantamento, fazendo uma análise de todos os dados comportados na organização e reconhecer se os princípios da lei e os direitos dos titulares estão sendo respeitados. (MOREIRA, 2021, p. 7)

3.2 SANÇÕES ADMINISTRATIVAS

Sabe-se que as sanções advindas da nova Lei decorrem dos danos causados pelo tratamento indevido dos dados pessoais. Dessa forma, passa-se a exigir dos controladores e operadores de dados, ou seja, daqueles que manuseiam os dados em caráter profissional, um dever de segurança. Presume-se que tais operadores sejam capacitados e qualificados o suficiente para garantir a integridade e preservação da privacidade de seus titulares. (MIRAGEM, 2019, p. 26)

Posto isto, para a concretização do nexo causal do dano, exige-se a falha do controlador ou do operador. Contudo, independente da falha se dar por dolo ou culpa, apenas sua constatação é suficiente para atribuição da responsabilidade. Além disso, há a possibilidade de inversão do ônus da prova em favor do titular dos dados, nas mesmas hipóteses de hipossuficiência e verossimilhança que a autorizam no âmbito das relações de consumo (art. 42, § 2º, da LGPD). (MIRAGEM, 2019, p. 26)

Segundo Bruno Miragem (2019, p. 26):

> O art. 44 da LGPD define que “o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I – o modo pelo qual é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.” A técnica legislativa empregada na LGPD aproxima-se notoriamente daquela adotada pelo CDC (LGL\1990\40) ao disciplinar o regime do fato do produto e do serviço, em especial na definição dos critérios a serem considerados para determinação do atendimento ao dever de segurança.

Diante disso, a LGPD previu a obrigação dos agentes de tratamento de dados (controladores e operadores) de adotarem boas práticas de governança, inclusive com a adoção de programas que atendam a requisitos mínimos definidos na legislação, sujeito a avaliação sobre sua efetividade (art. 50). (MIRAGEM, 2019, p. 15)

Ante o exposto, as sanções aplicadas poderão variar de acordo com o ato praticado, com possibilidade de imposição de multa com um teto de 50 milhões. Isabella Pompilio (2020) afirma que as penalidades variam desde advertências e multas, até à suspensão ou proibição, parcial ou total, do exercício de atividades relacionadas ao tratamento de dados, podendo significar, inclusive, o encerramento da própria atividade empresarial para algumas organizações.

Segundo o advogado especialista em proteção de dados, Enrique Tello Hadad (2021):

> As penalidades administrativas são aplicadas pela ANPD, podendo variar de acordo com o grau do impacto e a gravidade da infração à LGPD, desde uma advertência a multas simples de até 2% do faturamento das empresas (limitadas a R$ 50 milhões por infração), multas diárias, publicização da infração, bloqueio ou eliminação de dados pessoais, suspensão e até a proibição parcial ou total das atividades das empresas.

Os artigos 52, 53 e 54 da Lei entraram em vigor no dia 1º de agosto de 2021 estabelecendo um rol variado de sansões administrativas:

> Art. 52 *(i)* advertência, com indicação de prazo para adoção de medidas corretivas; *(ii)* multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu

> último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; *(iii)* multa diária, observado o limite total a que se refere o inciso II; *(iv)* publicização da infração após devidamente apurada e confirmada a sua ocorrência; *(v)* bloqueio dos dados pessoais a que se refere a infração até a sua regularização; *(vi)* eliminação dos dados pessoais a que se refere a infração; *(vii)* suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; *(viii)* suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; *(ix)* proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (BRASIL, 2018)

O site oficial do Governo Federal esclarece que a Lei Geral de Proteção de Dados determina que a ANPD (Agencia Nacional de Proteção de Dados) deverá editar regulamento próprio sobre sanções administrativas. Estas deverão ser objeto de consulta pública, contendo as metodologias que orientarão o cálculo do valor-base das sanções de multa. (SANÇÕES, 2021)

Dessa forma, as metodologias para as sanções pecuniárias devem ser anteriormente publicadas e expor precisamente os moldes e dosimetrias para o cálculo do valor-base das sanções de multa, que deverão conter fundamentação detalhada de todos os seus elementos, demonstrando a observância dos critérios previstos na LGPD. (SANÇÕES, 2021)

Dessa forma, é aberto ao público como se perfaz a análise para se chegar ao valor da multa de cada caso concreto:

> Nos termos da Lei, a aplicação de sanções requer, ainda, criteriosa apreciação e ponderação de diversas circunstâncias, dentre as quais a gravidade e a natureza das infrações e dos direitos pessoais afetados, a condição econômica do infrator, o grau do dano, a cooperação do infrator, a adoção de política de boas práticas e governança e a pronta adoção de medidas corretivas. (SANÇÕES, 2021)

A ANPD, órgão fiscalizador da nova Lei é a única organização que detém competência para aplicar as sanções administrativas supramencionadas. Assim, no que tange à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública, a Agência Nacional de Proteção de Dados prevalece hierarquicamente. (LGPD, 2021)

> Vale lembrar, entretanto, que, nos termos da Lei, a aplicação das sanções previstas na LGPD não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor) e em legislação específica. Assim, eventual atuação de outros órgãos públicos, como agências reguladoras ou órgãos de defesa do consumidor, deve se dar segundo as suas próprias competências, ao abrigo de suas legislações específicas. (GOVERNO, 2021)

Portanto, tem-se que o papel de uma autoridade de proteção de dados no ambiente de uma sociedade digital, tendo em vista que o RGPD, em vigor na União Europeia, e a LGPD, no Brasil, demonstram uma caminhada humanitária em direção à ampliação do universo protetivo dos dados pessoais. Porém, pode-se relevar insuficiente sem a apreensão do contexto de uma sociedade remodelada, com novas dinâmicas, e que, portanto, demanda novas formas de enfrentamento do problema de violação direta ou invisível de direitos. Uma delas reside em levar a constituição, estruturação, planejamento da ANPD, compatível com a realidade e ascensão das transformações da sociedade em rede. (SZINVELSKI, 2021)

3.3 CUSTOS E RISCOS

É evidente que a adequação à LGPD gerou e está gerando custos sobressalentes ao setor empresarial, sobretudo no contexto brasileiro em que as micro e médias empresas, em sua maioria, se veem com dificuldades financeiras e enfrentam a falta de subsídio para a implementação de consultorias, sistemas, especializações, dentre outros encargos, que variam mediante o porte, perfil e atividade da instituição.

Neste sentido, de acordo com a pesquisa feita pela Serasa Experian, realizada um ano antes da vigência da Lei, em agosto de 2019, cerca de 85% das empresas brasileiras não estavam preparadas para atender às exigências da LGPD. A pesquisa foi realizada com 508 empresas do país, de 18 setores de atuação distintos e de portes variados. (FUMOS, FREITAS, EVANGELISTA, 2019)

Entretanto, é necessário ponderar que os riscos iminentes de um vazamento de dados são incalculáveis, e podem comprometer gravemente e de forma irreversível

a imagem do negócio. De acordo com uma pesquisa realizada pelo National Cyber Security Alliance[3], 25% das pequenas e médias empresas declaram falência após um incidente de proteção de dados. (FARINHA, 2021)

Segundo o Relatório de Custo da Violação de Dados da IBM Security, sobre o impacto financeiro das violações de dados nas empresas, uma violação custa, na média global, US$ 3,8 milhões para as instituições. De acordo com o mesmo estudo, incidentes nos quais os atacantes acessam a rede das corporações com credenciais comprometidas ou roubadas tornam o custo de uma violação de dados ser quase US$ 1 milhão mais alto, chegando a US$ 4,77 milhões. (IBM, 2021)

A pesquisa realizada em 2020 ainda apontou que, no Brasil, esse custo médio da violação de dados corresponde a R$ 5,88 milhões. Globalmente, a indústria de saúde continua apresentando os mais altos custos médios de violação, com US$ 7,13 milhões — um aumento de mais de 10% em comparação com o estudo de 2019. Conclui-se que a não adequação do setor empresarial à LGPD é insustentável à sobrevivência de empresas, diante de valores exorbitantes. (IBM, 2021)

Em vista disso, se faz importante salientar que estar em consonância com a Lei, representa, ainda, um diferencial competitivo para as organizações. Isto é, as empresas que não se adequaram estão sujeitas a perder contratos, parcerias, clientes e oportunidades de negócios. Ou seja, o ônus oriundo da não conformidade com a Lei vai além do bloqueio das informações e das multas. (FARINHA, 2021)

Ainda, um estudo realizado pelo Instituto Ponemon, indica que o risco que uma empresa brasileira tem de sofrer um ataque cibernético é de 43%, muito superior ao de países que possuem uma cultura de segurança digital, como Alemanha (14%) e Austrália (17%). Isso porque, além de se adequar à lei é necessário criar, de fato, uma cultura corporativa de proteção e segurança dos dados. Portanto, o obstáculo não é apenas ajustar-se, mas sim, manter-se em conformidade com a legislação. (PONEMON, 2020)

[3] A National Cyber Security Alliance, uma organização 501 sem fins lucrativos fundada em 2001, é uma parceria público-privada sem fins lucrativos sediada nos Estados Unidos que promove a educação e a conscientização sobre segurança cibernética e privacidade.

O primeiro secretário da ACICG (Associação Comercial e Industrial de Campo Grande), Roberto Oshiro, explica que uma micro ou média empresa que deseje se adequar corretamente à LGPD deverá, primeiramente, contratar uma assessoria para fazer um “raio-x” dos procedimentos do negócio e elaborar os termos de consentimento. Deverão ser analisados como os cadastros dos clientes fornecedores são colhidos, como os funcionários captam as informações, onde elas são guardadas, o que é feito com esses dados, etc. (CAMPOS, 2020)

Oshiro (2020) entende que “o melhor é ter o banco de dados em nuvem. Empresas como Google, Amazon se responsabilizam pela segurança, se alguma coisa vazar, por exemplo, elas podem ser acionadas por isso e isso tem um preço”.

CONCLUSÃO

Ante todo o exposto, conclui-se que as inovações advindas do progresso tecnológico transformaram o modo que as informações são usadas e compartilhadas. O progresso dos meios de comunicação criou uma rede de compartilhamento de dados pelo mundo, de forma que os dados pessoais e sensíveis dos indivíduos correm a todo vapor, de forma nunca vista antes. Diante disso, entendeu-se pela necessidade de regulamentar e intermediar o compartilhamento e manuseio dessas informações.

O presente trabalho baseou-se no estudo acadêmico do Direito Digital conjuntamente com o Direito Constitucional e a tutela pelos direitos fundamentais dos indivíduos. Ademais, foi realizada uma intensa pesquisa acerca da proteção de dados no Brasil e na Europa, de maneira a entender os impactos da nova lei no contexto empresarial brasileiro.

Verificou-se que a adequação das empresas à Lei Geral de Proteção de Dados é indispensável para o bom funcionamento destas. Além de trazer maior segurança aos titulares dos dados, a implantação da nova Lei será primordial para a reputação e proteção das instituições, havendo uma certa equiparação legal do mercado brasileiro com os demais existentes no contexto mundial, e proporcionando uma relação mais transparente e confiável com o cliente.

Ademais, por mais que tal adequação ao novo regulamento traga custos à atividade empresarial, os ônus oriundos do descumprimento das normas são maiores. Isto é, as multas fixadas pela Lei podem chegar em até R$ 50 milhões (cinquenta milhões de reais). Além disso, com a aplicação da norma, as empresas se previnem de ataques cibernéticos e garantem uma boa reputação diante dos seu público.

Portanto, apesar dos obstáculos enfrentados pela atividade empresarial no caminhar da adequação à Lei Geral de Proteção de Dados, é inegável que, a longo prazo, os impactos da Lei beneficiam fortemente as instituições e a sociedade.

BIBLIOGRAFIA

ANDRADE, Jade; STEPENOSKI, Patrícia. **Lei Geral de Proteção de Dados**: impactos negativos e positivos – A necessária adequação por parte das empresas. Disponível em: <http://bpoadvogados.com.br/lei-geral-de-protecao-de-dados-impactos-negativos-e-positivos-a-necessaria-adequacao-por-parte-das-empresas/#_ftn1>. Acesso em: 10/10/2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, [2016]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 out. 2021

BRASIL. **Lei no 13.709, de 14 de Agosto de 2018**. Brasília, DF: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 16 out. 2021

BRASIL. **Lei no 10.406, de 10 de Janeiro de 2002**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm Acesso em: 29/10/2021

BEZERRA, Maria Ruth Borges. **Autoridade nacional de proteção de dados pessoais:** a importância do modelo institucional independente para a efetividade da lei. 2019. 95 f. TCC (Graduação) - Curso de Direito, Escola de Direito e Administração Pública do Idp, Brasilia, 2019.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: A função e os limites do consentimento. São Paulo: Forense, 2019.

BLUE PHOENIX. “Boas práticas de segurança”. Disponível em: www.bluephoenix.org. Acessado em: 25/10/2021

BODIN DE MORAES, Maria Celina. **LGPD**: um novo regime de responsabilização civil dito “proativo”. Editorial à Civilistica.com. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>. Acesso em: 11/11/2021.

CÂMARA, Flávia da Silva. **Lei Geral de Proteção de Dados Pessoais (LGPD) – aplicada às empresas de Contabilidade**. 2020. 50f. Trabalho de Conclusão de Curso (Graduação em Ciências Contábeis) – Departamento de Ciências Contábeis, Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2020.

CAMPOS, Ricardo. **Quanto custa para uma micro ou média empresa se adequar às normas da LGPD?**. Disponível em: https://correiodoestado.com.br/economia/quanto-custa-para-uma-empresa-se-adequar-a-lgpg/376505. Acesso em: 24/10/2021.

CANDIDO, João Pedro Succi; ARAÚJO, Tayná Frota; RIBEIRO, William Alves Carvalho. **Histórico da Lei Geral de Proteção de Dados (LGPD)**. Disponível em: <https://advocatta.org/historico-da-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 20/09/2021.

CERVO, Amado Luis; BERVIAN, Antônio. **Pesquisa em ciências humanas e sociais**. 5. ed. São Paulo: Cortez, 2001.

CHAVES, Natália Cristina; GUIMARÃES, Lucas Badaró. **Lei geral de proteção de dados:** o alerta aos empresários persiste em tempos de pandemia. Disponível em: <https://www.migalhas.com.br/depeso/324907/lei-geral-de-protecao-de-dados--o-alerta-aos-empresarios-persiste-em-tempos-de-pandemia>. Acesso em: 12/10/2021.

DONEDA, Danilo. O direito fundamental à proteção de dados pessoais. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coords.) **Direito digital, Direito privado e internet**. 2. ed. Indaiatuba: Foco, 2020.

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

DUQUE, Bruna Lyra; PEDRA, Adriano Sant'Ana. Os deveres fundamentais e a solidariedade nas relações privadas. **Revista de Direitos Fundamentais e Democracia**, Curitiba, v. 14, n. 14, p. 147-161, julho/dezembro de 2013.

ENTENDA o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1**, Rio de Janeiro, 20 mar. 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml >. Acesso em: 18/09/2021.

FUMO, Marianna; FREITAS, Brunna; GREGHI, Ana; EVANGELISTA, Viviane. 85% das empresas declaram que ainda não estão prontas para atender às exigências da Lei de Proteção de Dados Pessoais. **Serasa Experian.** 08 de agosto de 2019. Disponível em: https://www.serasaexperian.com.br/sala-deimprensa/85-das-empresas-declaram-que-ainda-nao-estao-prontas-para-atender-as-exigencias-da-lei-deprotecao-de-dados-pessoais-mostra-pesquisa-da-serasa-experian. Acesso em: 24/10/2021.

FARINHA, Marcelo. LGPD: custo ou investimento?. **Diário do Comércio**. Belo Horizonte. 20 maio 2021. Disponível em: <https://diariodocomercio.com.br/opiniao/lgpd-custo-ou-investimento>. Acesso em: 12/10/2021.

GONZALES, Mariana. **LGPD Comentada**. 2019. Disponível em: <https://guialgpd.com.br/lgpd-comentada/>. Acesso em: 03/11/2021

HOME | PONEMON INSTITUTE. **Ponemon Institute**. Disponível em: <https://www.ponemon.org/>. Acesso em: 12 nov. 2021.

KÖCHE, José Carlos. **Fundamentos de metodologia científica:** teoria da ciência e prática da pesquisa. 14. ed. rev. amp. Petrópolis, RJ: Vozes, 1997.

LEAL, Rhand. **O que é a ISO 27001**. Disponível em: https://advisera.com/27001academy/pt-br/o-que-e-a-iso-27001/. Acesso em: 17 out. 2021.

LIMBERGER, Têmis. Proteção dos dados pessoais e comércio eletrônico: os desafios do século XXI. **Revista de Direito do Consumidor**, São Paulo, ano 17, n. 67, p. 218, jul.-set. 2008.

LGPD: Lei Geral de Proteção de Dados. **Governo Federal**. Disponível em: <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd>. Acesso em: 12/10/2021

LGPD: revisão dos principais pontos da lei de proteção de dados. **aDoc**, Porto Alegre, 28 ago. 2021. Disponível em: <https://adoc.com.br/lgpd-revisao-pontos-principais/>. Acesso em: 25/10/2021.

MARQUES, Cláudia L; BEJAMIN, Antonio, H. V.; BESSA, Leonardo, R. **Manual de Direito doConsumidor.** 6ª ed. rev. atual. São Paulo: Editora Revista dos Tribunais, 2014. p. 98 e 99.

MATOS, Tatiani Cristina. **Aspectos relevantes sobre a Lei Geral de Proteção de Dados Pessoais**. 23 mar. 2021. Disponível em: <https://conteudojuridico.com.br/consulta/artigos/56283/aspectos-relevantes-sobre-a-lei-geral-de-proteo-de-dados-pessoais>. Acesso em: 03/10/2021

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, v. 120. São Paulo: Ed. RT, nov.-dez. 2018, p. 469-483

MENDES, Laura Schertel. Privacidade**, proteção de dados e defesa do consumidor**: Linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MACIEL, Rafael Fernandes. **Manual prático sobre a lei geral de proteção de dados pessoais (Lei no 13.709/18)**. 1 Ed. Goiânia: RM Digital Education. 2019.

MARQUES, Cláudia Lima; BEJAMIN, Antonio, Herman de Vasconcellos; BESSA, Leonardo, Roscoe. **Manual de Direito do Consumidor**. 6a ed. rev. atual. São Paulo: Editora Revista dos Tribunais, 2014.

MINAYO, Maria Cecília de Souza. **O desafio do conhecimento:** pesquisa qualitativa em saúde. 4. ed. São Paulo/Rio de Janeiro: HUCITEC/ ABRASCO, 1996.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor.** In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (Coords.). Responsabilidade civil e novas tecnologias. Indaiatuba: Foco, 2020.

MONTINI, Nathalia Rosa. **Necessidade imediata de consolidação da ANPD para efetividade da LGPD e prevenção de excessivas demandas judiciais**. Monografia – Direito. Faculdade de Ciências Jurídicas e Sociais – FAJS (UniCEUB). Brasília. 2020

MOREIRA, Natanael de Jesus. **Lei geral de proteção de dados pessoais:** a adaptação das empresas prestadoras de serviços contabéis da região sul catarinense. Monografia - Ciências Contábeis, Universidade do Extremo Sul Catarinense, UNESC. Criciúma. 2021.

MOREIRA, Nelson Camatta. Constitucionalismo Dirigente no Brasil: em busca das promessas descumpridas. **Revista de Direitos e Garantias Fundamentais**, Vitória, n. 3, p. 87-128, jul./dez. 2008. DOI: https://doi.org/10.18759/rdgf.v0i3.54. Disponível em: <https://sisbib.emnuvens.com.br/direitosegarantias/article/view/54>. Acesso em: 12/10/2021.

NASCIMENTO, Leticia. **Os principais direitos fundamentais garantidos na Lei Geral de Proteção de Dados Pessoais**. Set. 2019. Disponível em:

<https://jus.com.br/artigos/76752/os-principais-direitos-fundamentais-garantidos-na-lei-geral-de-protecao-de-dados-pessoais>. Acesso em: 12/10/2021.

O que são dados pessoais?. **Comissão Europeia**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_pt. Acesso em: 12/10/2021

PANEK, Lin Cristina Tung. **Lei Geral de Proteção de Dados nº 13.709/2018**: Uma análise dos principais aspectos e do conceito privacidade na sociedade informacional. 2019. Trabalho de Conclusão de Curso (Graduação em Direito). Universidade Federal do Paraná. Curitiba. 2019.

PEDRA, Adriano Sant'Ana. **A Constituição viva:** poder constituinte permanente e cláusulas pétreas na democracia participativa. Rio de Janeiro: Lumen Juris, 2014.

PEDRA, Adriano Sant'Ana. **A Constituição viva:** poder constituinte permanente e cláusulas pétreas na democracia participativa. Rio de Janeiro: Lumen Juris, 2012.

PEREIRA, Marcelo Cardoso. **Direito à intimidade na internet**. Curitiba: Juruá, 2004.

PESTANA, Márcio. **Os princípios no tratamento de dados na LGPD (Lei Geral da Proteção de Dados Pessoais**. 2020. Disponível em: <https://www.conjur.com.br/dl/artigo-marcio-pestana-lgpd.pdf>. Acesso em: 12 Out. 2021.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (lgpd). 2. ed. São Paulo: Saraiva Educação, 2020. 152 p.

PINHEIRO, Victor Sales; BONNA, Alexandre Pereira. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito. **Revista Direito e Garantias Fundamentais**, Vitória, v. 21, n. 3, p. 365-394, set./dez. 2020.

REINALDO, Demócrito. **Direito da informática:** temas polêmicos. Bauru/SP: EDIPRO, 2002.

RODOTÁ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008

RICARDO, Sérgio. **A regulação jurídica da proteção de dados pessoais no Brasil**. Monografia de pós graduação – Curso de Direito da propriedade intelectual da PUC- Rio, Pontifícia Universidade Católica do Rio de janeiro. Rio de Janeiro, 2018.

RIBEIRO, L. **Proteção de dados pessoais:** Estudo comparado do regulamento 2016/679 do parlamento europeu e conselho e o projeto de lei brasileiro n. 5.276/2016. Brasília, p. 5 – 24, 2016.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada:** uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte. Belo Horizonte: Del Rey, 1998. p. 493

SANÇÕES Administrativas: o que muda após 1º de agosto de 2021?. **Governo Federal**. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em 10/10/2021.

SILVA, Evelyn. **O que é a lei geral de proteção de dados (LGPD)**. 2021. Disponível em: <https://schmallesilva.com.br/o-que-e-a-lei-geral-de-protecao-de-dados-lgpd/>. Acesso em: 12/10/2021.

SILVA, Ricardo Baretto; BRANCHER, Paulo; TALIBERTI, Camila; CUNHA, Vitor. **Entra em vigor o Regulamento Geral de Proteção de Dados da União Europeia**. 2018. Disponível em: <https://www.migalhas.com.br/depeso/281042/entra-em-vigor-o-regulamento-geral-de-protecao-de-dados-da-uniao-europeia>. Acesso em: 14/10/2021

STRICKLAND, Fernanda; ICARO, Pedro. **Sanções da LGPD estão em vigor e instituições devem ficar atentas às novas normas**. 2021. Disponível em: <https://www.correiobraziliense.com.br/politica/2021/08/4941113-sancoes-da-lgpd-entram-em-vigor-e-instituicoes-devem-ficar-atentas-as-novas-normas.html>. Acesso em: 02/11/2021.

SZINVELSKI, Martin Marks. **O Direito à Proteção de dados na sociedade em rede:** a perspectiva comparada entre a Autoridade Nacional de Proteção de Dados (ANPD) e a Unidade Reguladora e Controladora dos Dados Pessoais (URCDP) do Uruguai. Dissertação (Mestrado em Direito Público) – Universidade do Vale do Rio dos Sinos – UNISINOS. São Leopoldo. 2021

TOSTES, Marcelo. **Segurança de dados na Internet:** como proteger a sua empresa?. 2019. Equipe Marcelo Tostes. Disponível em:

https://transformacaodigital.com/juridico/segurancade-dados-na-internet-como-proteger-a-sua-empresa/. Acesso em: 03 out. 2021.

VIEIRA, T.M. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Dissertação (Mestrado em Direito). Universidade de Brasília, Brasília, 2007.

WACHOWICZ, Marcos. **A proteção jurídica das bases de dados em face da revolução da tecnologia da informação**. Artigo atualizado e originalmente publicado na revista de direito autoral, São Paulo, v. iii, 2005.

ZANON, João Carlos. **Direito à Proteção dos Dados Pessoais**. São Paulo, Revista dos Tribunais, 2013.