UNIVERSIDADE FEDERAL DO CEARÁ

FACULDADE DE DIREITO

BACHARELADO EM DIREITO

LUÍS EDUARDO GUEDES COLÁCIO

OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS SOB A ÓTICA EMPRESARIAL

FORTALEZA

2025

LUÍS EDUARDO GUEDES COLÁCIO

OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS SOB A ÓTICA EMPRESARIAL

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Carlos César Sousa Cintra.

FORTALEZA

2025

Dados Internacionais de Catalogação na Publicação Universidade Federal do Ceará
Sistema de Bibliotecas Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C642i Colácio, Luís Eduardo Guedes.

OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS SOB A ÓTICA EMPRESARIAL:

Estudo exploratório / Luís Eduardo Guedes Colácio. – 2025.

51 f.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito,

Curso de Direito, Fortaleza, 2025.

Orientação: Prof. Dr. Carlos César Sousa Cintra.

Coorientação: Prof. Me. José Eduardo Barroso Colácio.

1. LGPD. 2. Dados pessoais. 3. Privacidade. 4. Proteção de dados. 5. Empresarial. I. Título.

CDD 340

LUÍS EDUARDO GUEDES COLÁCIO

OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS SOB A ÓTICA EMPRESARIAL

Monografia apresentada ao Curso de Graduação em Direito da Universidade Federal do Ceará como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovada em: 14 / 07 / 2025

BANCA EXAMINADORA

_____
Prof. Dr. Carlos César Sousa Cintra (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Lucas Antunes Santos
Universidade Federal do Ceará (UFC)

_____
Profa. Dra. Isabelly Cysne Augusto Maia
Unichristus (membro externo)

Dedico este trabalho acima de tudo a Deus, a minha família e a amigos que sempre me apoiaram.

AGRADECIMENTOS

A jornada para a conclusão desta monografia foi repleta de desafios, aprendizados e superações. Assim, este trabalho não seria possível sem o apoio, a dedicação e a inspiração de muitas pessoas às quais expresso minha mais profunda gratidão.

A Deus, pela força, pela saúde e pelas oportunidades concedidas ao longo dessa caminhada.

À minha família, pelo amor incondicional, pelo incentivo constante e pela paciência nos momentos de dificuldades. Vocês foram meu alicerce e minha maior motivação para seguir em frente. Em especial, exponho os meus mais sinceros e profundos agradecimentos aos meus pais, José Eduardo Barroso Colácio, meu pai que é a maior referência e inspiração dentro de qualquer seara profissional e acadêmica de minha vida, além de ser um exemplo de ética e virtude, e Eneida Porcina Guedes Colácio, minha mãe que é e sempre será a minha maior fonte de amor verdadeiro e inspiração, que sempre me motivou a procurar ser a minha melhor versão, e ao meu único irmão, Daniel Guedes Colácio, o meu maior exemplo de disciplina e evolução, que sempre esteve ao meu lado, crescendo em todos os aspectos da vida juntos, dedico a estas pessoas, que nunca desistiram de mim, mesmo nos momentos mais desafiadores da minha caminhada, e sempre estiveram ao meu lado para me apoiar e pavimentar o meu caminho para o sucesso, sem o apoio de vocês jamais teria conseguido alcançar meus objetivos.

Aos meus amigos, que estiveram ao meu lado em todas as fases dessa trajetória acadêmica, compartilhando conhecimentos, desafios e momentos de descontração que tornaram essa jornada mais leve.

Aos meus professores, que, com dedicação e excelência, contribuíram para minha formação acadêmica e intelectual. Em especial, agradeço ao meu orientador, Prof. Dr. Carlos César Sousa Cintra, por sua paciência, incentivo e valiosas contribuições, que foram essenciais para a construção deste trabalho.

À Universidade Federal do Ceará, pela estrutura e pelos ensinamentos que proporcionaram minha evolução pessoal e profissional, preparando-me para os desafios da vida jurídica.

A todos que, direta ou indiretamente, contribuíram para a realização deste trabalho, meu sincero muito obrigado.

O mistério da vida não é um problema a ser resolvido, mas uma realidade a ser vivenciada. (Frank Herbert).

RESUMO

Muito vem sendo discutido sobre a proteção e privacidade de dados pessoais que estão sendo coletados e tratados por empresas, principalmente com os avanços da tecnologia. A fim de melhor proteger os titulares desses dados, a lei vem se transformando e evoluindo para ser aplicada em todos os países. Frente a esse contexto, tem-se o seguinte objetivo geral: investigar como a Lei Geral de Proteção de Dados vai impactar as relações empresariais, comerciais e consumeristas, sendo como objetivos específicos: Verificar como a Lei Geral de Proteção de Dados vai funcionar na prática; Verificar como a Lei Geral de Proteção de Dados pode ser eficaz na proteção de dados; Indicar quais são os maiores desafios para a fiel execução da Lei Geral de Proteção de Dados. Para alcançar essas propostas a metodologia fundamentou-se em uma revisão bibliográfica e documental em que foram consultados livros, revistas, artigos científicos que tiveram como base os conhecimentos de alguns autores, dentre eles Nakata (2019), Peck (2021), Limberger (2016); Santos (2012), dentre outros que abordam a temática em estudo. Ao final do estudo foram apresentadas as principais considerações sobre o tema explanado.

Palavras-chave: lei geral de proteção de dados; empresa; relações consumeristas.

ABSTRACT

There has been much discussion about the protection and privacy of personal data that has been collected and processed by companies, especially with advances in technology. In order to better protect the holders of these data, laws have been applied in all countries. In this context, the following general objective is to investigate how the General Data Protection Law will impact business, commercial and consumer relations, with the following specific objectives: To verify how the General Data Protection Law will work in practice; To verify how the General Data Protection Law can be effective in protecting data; To indicate what are the biggest challenges for faithful implementation of the General Data Protection Law. To achieve these proposals, the methodology was based on a bibliographic and documentary review in which books, magazines, and scientific articles were consulted, based on the knowledge of some authors, including Nakata (2019), Peck (2021), Limberger (2016); Santos (2012), among others who address the topic under study. At the end of the study, the main considerations on the topic explained were presented.

Keywords: general data protection law; company; consumer relations.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Autoridade Nacional de Proteção de Dados
APLPD	Anteprojeto de Lei de Proteção de Dados
DPO	Data Protection Officer
GDPR	General Data Protection Regulation
ISO	*International Organization for Standardization*
LGPD	Lei Geral de Proteção de Dados
RGPD	Regulamento Geral de Proteção de Dados
SAFARI	*Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus*

SUMÁRIO

1 INTRODUÇÃO

Em um panorama global, em que o crescimento e a dependência tecnológica vêm crescendo cada vez mais, nos levando a maiores situações de riscos, com o grande número de vazamento de dados pessoais, no século XXI é evidente que a quantidade de informações produzidas todos os dias na internet é exorbitante, sites, redes sociais, e-mails dentre outras. O vazamento e a utilização indevida de dados têm se tornado um problema cada vez mais frequente na população global, gerando várias consequências para aqueles que foram expostos, ferindo e violando a intimidade.

A utilização indevida e o vazamento de dados pode gerar consequências perenes, visto que uma vez vazado dos sistemas, podem vir a prejudicar de forma financeira e moral os usuários. Com isso, aspectos que são referentes as estratégias de sistemas que sejam sigilosos podem comprometer as ações e prejudicar o andamento de vários processos. Além disso, transações bancárias também são afetadas, já que contas e valores são expostos para terceiros.

Na comunicação e no mercado empreendedor, o vazamento dessas informações contribui para uma imagem negativa de diversas empresas, expondo a credibilidade e afetando o mercado digital negativamente. Isso pode ocorrer, principalmente, se a população for diretamente afetada, o que pode demonstrar o descuido com a segurança digital de uma empresa.

Alguns exemplos que foram divulgados na mídia mostraram bem a dimensão desses prejuízos, como, por exemplo, o que aconteceu com Facebook, que expõe bem a proporção dos riscos de vazamento de dados. A empresa então anunciou em 2018 que aproximadamente 50 milhões de usuários da rede foram afetados com o vazamento de dados pessoais. Tal problema indica que há uma falha no controle desses dados, o que colaborou para evidenciar a vulnerabilidade no tratamento de dados, contribuindo para a formação de uma imagem negativa da empresa para o público.

Além disso, de acordo com o estudo *From data boom to data doom: the risks and rewards of protecting personal data*, realizado, em 2018, pela *Kapersky Lab*, acidentes envolvendo vazamento de dados resultam na demissão no mercado dos profissionais envolvidos. Entre os casos analisados no estudo, 29% dessas demissões foram de pessoas que ocupavam cargos de alto escalão em pequenas e médias empresas e 27% em grandes corporações (Softwall, 2019).

Outro ponto que merece destaque é a negligência em diversos casos que as empresas podem ter hoje com a prevenção e o cuidado com a segurança dos dados de seus clientes, frente a legislação atual de proteção de dados. O consumidor terá uma maior facilidade

em reivindicar e receber indenizações dessas empresas que negligenciam o cuidado com seus dados. Muito dessas pessoas jurídicas por visualizarem suas vendas e expansão de mercado em constante crescimento, principalmente por conta do mercado digital, ao dispor dessa ferramenta cada vez mais presente, deixam de lado a organização de manter a privacidade e os dados íntimos de seus clientes em segurança.

Vale ressaltar que, o vazamento de dados pessoais atinge proporções, ainda, para ser um problema de repercussões à administração pública, como, por exemplo, em meados de 2019, quando ocorreu o famoso caso do Ministro Sérgio Moro, em que um hacker teve acesso a conversas íntimas e as soltou na imprensa com o intuito de ferir a dignidade e manchar a imagem dele, assim como diversas outras vítimas de imagem pública notória foram prejudicadas, conforme a Operação da Polícia Federal intitulada de "*Spoofing*". Esse tipo de incidente cresceu aproximadamente mais de 19 vezes em um espaço tempo de seis anos e tornou-se o segundo maior tipo de ataque cibernético sofrido pelos sistemas do Governo Federal, conforme estatísticas levantadas pela Polícia Federal.

Observa-se assim, que o atual panorama sobre a regulamentação das políticas voltadas para o uso de dados, vem evidenciando o surgimento de tendências globais inovadoras, com expressivas mudanças no sistema jurídico de vários países, que tem como principal propósito estabelecer claras e objetivas diretrizes em direção a privacidade e segurança.

Nesse contexto, destaca-se a Lei Geral de Proteção de Dados (Nº 13.709 de 2018), que em agosto completará sete anos que foi aprovada, estabelecendo e inovando regras para as ações de coleta e tratamento de informação de dados, seja de dados pessoais, de empresas ou de instituições públicas.

Com a instituição da referida lei no país, o Brasil passou a não apenas fazer parte dos países que possuem leis específicas focadas na proteção de dados pessoais, sanando as lacunas deixadas em mais de 40 diplomas legais, substituindo e/ou complementando a estrutura existente à época, de forma esparsa, regulamentando o uso e tratamento de dados no atual cenário do país. Destarte, importante destacar que a LGPD, no contexto global, ainda se apresenta como sendo um modelo de regulamentação referência para o mundo, sendo reconhecida em diversos países como modelo no tratamento de dados pessoais.

A partir do exposto, buscar-se-á desenvolver pesquisa monográfica que responda aos seguintes questionamentos: Como a Lei Geral de Proteção de Dados (LGPD) impacta na forma que as empresas lidam com os dados pessoais de seus clientes? Qual é o maior desafio do Governo Federal na fiscalização e na efetividade da LGPD? Como operacionalizar com eficiência e segurança o tratamento de dados sigilosos?

Como objetivo geral, pretende-se investigar como a LGPD impacta as relações empresariais, comerciais e consumeristas. Para tanto foram estabelecidos os seguintes objetivos específicos: Verificar como a LGPD funciona na prática; Verificar como a LGPD pode ser eficaz na proteção de dados; e, indicar quais são os maiores desafios para fiel execução da LGPD. Para alcançar a proposta estabelecida para o estudo, a metodologia fundamentou-se em uma revisão bibliográfica, tendo como base os ensinamentos de Alexandre Nakata (2019), Têmis Limberger (2016); Patrícia Peck Pinheiro (2021), dentre outros que abordam a temática em estudo.

O trabalho está estruturado em mais quatro capítulos e a conclusão. No primeiro capítulo, discute-se a importância e conceituação da Lei Geral de Proteção de Dados, evidenciando os principais pontos relativos à efetividade. Discorre-se sobre a Proteção de Dados pessoais como um direito fundamental e a promulgação da Emenda Constitucional 115/2022.

No segundo capítulo é feita uma explanação sobre a normativa europeia de proteção de dados e as repercussões das discussões e marcos legais no direito brasileiro. Em relação ao terceiro capítulo apresenta-se a interface da LGPD: o escopo da construção do direito à proteção de dados. O quarto capítulo explana sobre os impactos da LGPD nas relações consumeristas e empresariais contemporâneas. Ao final, são descritas as principais considerações e sugestões para pesquisas futuras.

2 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

Com a crescente globalização vivenciada, em especial, com o intenso advento e uso da tecnologia por parte das pessoas físicas e jurídicas, surgiu a necessidade de efetivar a proteção da pessoa humana nos meios digitais, por meio da administração e proteção de forma limpa e clara dos dados utilizados em operações de qualquer natureza no âmbito da tecnologia, tornando a proteção do cidadão, dos dados pessoais e o direito à privacidade destes um direito fundamental inerente à pessoa humana.

A grande quantidade e volume de dados gerados atualmente é assustadora, de maneira que bilhões de informações são originadas globalmente, uma vez que existem muitos meios que estão capturando, processando e armazenando novos dados, como exemplo os Apps, Sistemas, TVs, Celulares e aparelhos com IoT (Internet of Things ou Internet das Coisas)[1].

Com isso, pode-se perceber a expansão do uso da internet por parte das pessoas, principalmente, por parte dos consumidores ao disponibilizarem os seus dados para efetivação de compras nos meios digitais. Nesse sentido, ressalta que anterior ao surgimento e vigência da Lei nº 13.709/2018 o tratamento dos dados utilizados nas operações digitais era realizado de forma descabida e desarrazoada, uma vez que os usuários aceitavam a manipulação dos seus dados por qualquer pessoa ou terceiro, ocasionando o que foi denominado de Big Data.

Fazendo uma breve análise, entende-se por Big Data o agrupamento de técnicas capazes de se analisar grandes quantidades de dados, ou ainda, o conjunto de dados coletados previamente e, ao serem reunidos acabam por formar o perfil de um indivíduo.

É importante ressaltar a vulnerabilidade dos cidadãos perante à tecnologia avançada e aos algoritmos, nos quais possuem a capacidade de manipular e induzir o que será visto pelos indivíduos nos sites e nos meios digitais em geral, por meio do rastreamento de interesses dos usuários, como exemplo disso são as mensagens publicitárias recebidas de lojas ou sites de intermediação de venda, as quais foram direcionadas a partir da coleta de informações realizadas pelos celulares e computadores utilizados, sendo essa, umas das infindas aplicabilidades que o Big Data realiza, utiliza-se desses dados coletados para fins econômicos.

Nesse contexto, conforme fora mencionado por Magro (2020), a utilização e influência de Big Data viabilizará o reconhecimento do indivíduo, qual seja titular de dados, e resultará na definição do perfil comportamental do usuário a partir dos seus interesses, fazendo

[1] Refere-se à rede coletiva de dispositivos conectados e à tecnologia que facilita a comunicação entre os dispositivos e a nuvem, bem como entre os próprios dispositivos.

com que este concorde sem que tenha tido a total compreensão do consentimento dado para tanto.

Assim, diante da fragilidade dos indivíduos frente à crescente utilização e advento dos meios digitais para diversas operações sejam elas consumeristas ou empresariais, restou clara a urgência de um processo de proteção dos dados, de forma a garantir e assegurar a inviolabilidade da privacidade nessa nova era, bem como, ainda, surgindo a necessidade de debater os problemas causados pela coleta descontrolada de dados pessoais e a consequente formação de Big Data com a finalidade principal de se chegar a uma solução viável para a problemática causada pelo seu uso indevido.

Portanto, neste capítulo serão elucidados e analisados os principais pontos relativos à proteção e tratamento dos dados pessoais em conformidade com a influência e implementação da Lei Geral de Proteção de Dados, bem como as principais motivações do Estado brasileiro a editar uma lei tratando especificamente de dados pessoais, e, ainda, relacionar a proteção de tais dados como um direito fundamental à pessoa humana.

2.1 A origem e evolução da Lei Geral de Proteção de Dados de nº 13.709/2018

Como se sabe o Direito é uma ciência onipresente e seus ditames também englobam a supervisão do mundo digital, uma vez que "internet não é terra sem lei", e assim, com o objetivo de disponibilizar aos usuários dos meios digitais uma segurança jurídica maior à sua privacidade e aos dados pessoais, o Estado brasileiro aprovou em 2014 a Lei n° 12.965, mais conhecida como Marco Civil da Internet, tratando-se de uma lei ordinária federal de iniciativa do Poder Executivo, consistente em um modelo de "Constituição da Internet", sendo sua principal finalidade o estabelecimento de princípios, garantias, direitos e deveres para o devido uso da internet e dos meios decorrentes desta no Brasil.

A lei em comento dispõe como princípios que devem ser elucidados para fins de análise e embasamento deste presente trabalho, nos termos em que serão mencionados nos tópicos seguintes, o princípio da proteção da privacidade e dos dados pessoais, conforme previsão do Art. 3º da Lei nº 12.965/2014:

> Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;

> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (Brasil, 2014).

Nesse sentido, ressalta-se que o Marco Civil da Internet assegura como direito e garantia dos indivíduos no âmbito digital a inviolabilidade e o sigilo das informações trocadas e das comunicações armazenadas, salvo por ordem judicial, assim depreende-se do entendimento do Art. 7º Lei nº 12.965/2014[2], pelo qual dispõe os direitos inerentes aos usuários (Brasil, 2014).

Com isso, depois do Marco Civil da Internet com influência e embasamento deste, a Lei Geral de Proteção de Dados (LGPD) de nº 13.709/2018 se tornou de um dos maiores avanços legislativos brasileiro referente à proteção dos dados e informações que circulam nos meios digitais.

Diante de diversos fatores, foi surgindo a necessidade de adequação da legislação brasileira, de modo que dispusesse de previsão acerca do asseguramento, tratamento e destinação dos dados pessoais dos indivíduos dentro do âmbito digital, considerando o grande volume e quantidade de dados pessoais que estão sendo armazenados na atualidade, bem como,

---

[2] "Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização; V - manutenção da qualidade contratada da conexão à internet; VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei e na que dispõe sobre a proteção de dados pessoais; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet". (Brasil, 2014).

após a influência e aprovação oficial do General Data Protection Regulation (GDPR) no ano de 2018 pela organização da União Europeia (UE).

O GDPR, cuida-se de um Regulamento Geral de Proteção de Dados (RGPD) (UE) 2016/679 do direito europeu versando sobre a privacidade e proteção de dados pessoais, a ser aplicado a todos os indivíduos na União Europeia e Espaço Econômico Europeu, devendo cada um dos 28 países da União Europeia obedecer fielmente ao que fora previsto.

Tal Regulamento, possui como finalidade principal proporcionar aos usuários das novas tecnologias a possibilidade de controlar os seus dados pessoais armazenados pelas empresas no ato de navegação na internet, tendo como principal preocupação a viabilidade em proporcionar a privacidade das pessoas e o cuidado com a segurança dos dados armazenados, possuindo as empresas a obrigação em solicitar o consentimento dos usuários para utilização dos seus dados pessoais, de modo que não haja o armazenamento de nenhuma informação que possa identificar um indivíduo sem a devida licença e autorização deste para tanto.

Além disso, o GDPR é bem claro ao dispor que a proteção das pessoas físicas em relação ao tratamento de dados pessoais é um direito fundamental, conforme podemos verificar em previsão do *General Data Protection Regulation (EU) 2016/679 of The European Parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive* 95/46/EC (*General Data Protection Regulation - Text with EEA relevance*), vejamos:

> The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her[3].

Como pode-se analisar, o Regulamento Geral de Proteção de Dados Pessoais Europeu foi o grande influenciador e ponto de partida para que o Estado Brasileiro prosseguisse com o estabelecimento de disposições acerca da proteção dos dados pessoais, e não é à toa que muitos dos conceitos concebidos pela LGPD foram, em muitos deles, concebidos do GDPR.

Com a finalidade de sanar tais lacunas e suprir a falta de legislação atinente ao assunto no ordenamento jurídico brasileiro, bem como, para impor regrar aos conflitos

[3] A proteção das pessoas físicas em relação ao tratamento de dados pessoais é um direito fundamental. O artigo 8.º, n.º 1, da Carta dos Direitos Fundamentais da União Europeia (a "Carta") e o artigo 16.º, n.º 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção da sua dados pessoais que lhe digam respeito.

envolvendo o tratamento de dados pessoais, foi necessário o advento e promulgação da LGPD. Corroborando com esse entendimento, vejamos o que evidencia Moraes e Queiroz:

> As noções tradicionais de privacidade e de divulgação mostram-se insuficientes e inadequadas diante das tecnologias presentes na sociedade da informação, demandando do intérprete um cuidadoso exame dos novos instrumentos para a proteção da pessoa humana no âmbito do tratamento dos dados pessoais. Com o advento da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), no contexto de assunção dos dados pessoais como bens jurídicos essenciais, assume relevo o direito à autodeterminação informativa como vetor de proteção dos dados pessoais. Quanto à responsabilização civil, um novo regime se faz presente. Cumpre investigar aqui sua potencialidade como instrumento de natureza multifuncional que apresenta, no que tange a danos causados pelos agentes de tratamento de dados, além da função comum compensatória, uma função de prevenção e dissuasão, vindo a criar, desse modo, um reforço para a garantia da proteção da privacidade dos dados pessoais (Moraes; Queiroz, 2019, p. 113).

Desta feita, pode-se observar as principais influências e embasamentos que deram suporte ao surgimento da LGDP no Brasil, bem como, ainda, a aproximação existente entre a legislação brasileira, ora em análise, com o Regulamento Europeu, a GDPR.

2.2 A análise dos principais pontos relativos à proteção e tratamento dos dados pessoais em conformidade com a implementação da Lei Geral de Proteção de Dados

A LGPD de nº 13.709/2018 encontra-se dividida em 10 capítulos, com 65 artigos, tendo alcance extraterritorial, ou seja, efeitos internacionais, possuindo como órgão federal fiscalizador e aplicador a Autoridade Nacional de Proteção de Dados (ANPD), pelo qual foi criada com atribuições em fiscalizar a devida aplicação da LGPD por parte das empresas, bem como, ainda, com a missão de divulgar como toda a informação pessoal e os demais dados pessoais utilizados pelas empresas devem ser tratados.

Com isso, cabe à ANPD fazer todo o auxílio de adequação e cumprimento da LGPD por parte das empresas, as quais devem preencher os requisitos legais e estabelecer as bases para os ajustes que devem ser propostos pelo órgão fiscalizador em comento. Ressalta-se que em caso de infração das disposições por não cumprimento e não adequação à LGPD, existem várias sanções que podem ser impostas, de uma simples advertência, ou, ainda, uma multa que pode chegar ao equivalente a 2% do faturamento do grupo econômico, valor este que será limitado à quantia de R$ 50.000.000,00, sem deixar de mencionar aqui, o consequente bloqueio e eliminação do banco de dados e armazenamento da empresa, conforme disposição expressa

do Art. 52 da LGPD, pelo qual dispõe como critério de aplicação alguns requisitos, em especial a proporcionalidade, vejamos:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> 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 - (VETADO);
>
> VIII - (VETADO);
>
> IX - (VETADO);
>
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Brasil, 2018).

Na sequência, comparada com o GDPR europeu, a LGPD apresenta uma proposta de atuação mais otimizada e, inclusive, como uma versão mais ampla das suas disposições, possuindo prazos razoáveis e mecanismos procedimentais eficazes, assim entende Patrícia Peck Pinheiro em seu livro sobre Proteção de Dados Pessoais: Comentários à Lei nº 13.709/2018 (LGPD):

> Portanto, a versão nacional é mais enxuta e em alguns aspectos deixou margem para interpretação mais ampla, trazendo alguns pontos de insegurança jurídica por permitir espaço para subjetividade onde deveria ter sido mais assertiva. Um exemplo disso ocorre em relação à determinação de prazos: enquanto o GDPR prevê prazos exatos, como de 72 horas, a LGPD prevê “prazo razoável”. (Pinheiro, 2021, p.11).

A LGPD possui como principal escopo de suas disposições aquelas situações em que há a possibilidade de realização do tratamento de dados pessoais, desde que obedecidas as terminações legais, para garantia da privacidade dos titulares, observadas as obrigações dos agentes de tratamento, a fim de que se tenha a segurança jurídica do interesse dos titulares e das informações disponibilizadas por estes.

Nesse contexto, é imperioso ressaltarmos e elucidarmos alguns pontos atinentes à LGPD, os quais são de extrema importância para o devido tratamento dos dados pessoais, analisando e ressaltando as suas terminações e conceituações legais, as quais serão dispostas nos próximos tópicos.

2.3 Conceitos e terminologias

Inicialmente, cabe evidenciarmos aqui que a LGPD predispõe em seus dispositivos todas as definições legais concernentes aos principais termos utilizados, uma vez que são fundamentais e devem ser objeto de disposições em documentos, como políticas de privacidade, Compromisso de Proteção de Dados, normas, procedimentos e contratos.

Nesse sentido, dados pessoais compreenderá quaisquer informações relacionadas a uma pessoa natural identificada ou identificável, ora titular a quem se referem os dados pessoais, os quais são objeto de algum tratamento, cuidando-se sempre de uma pessoa física, natural. Por conseguinte, ressalta-se que os dados pessoais estão relacionados as informações como nome, sobrenome, apelido, idade, endereço residencial ou eletrônico, cabendo incluir dados de localização, placas de automóvel, dados acadêmicos, sempre relacionados a uma pessoa natural.

A redação do Art. 5º, inciso I da LGPD propõe a conceituação legal ao que esse refere dado pessoal, conforme vejamos abaixo: “Art. 5º. Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;” (Brasil, 2018).

Quanto ao tratamento dos dados, conforme é previsto pelo Art. 5º, inciso X[4] da supramencionada lei, cuida-se da operação realizada com a finalidade de manusear os dados pessoais, como exemplo: a coleta, distribuição, produção, armazenamento, recepção, classificação, processamento, utilização, acesso, reprodução, transmissão, arquivamento,

[4] Art. 5º Para os fins desta Lei, considera-se: X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (Brasil, 2018).

edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, ou ainda, trata-se de qualquer operação ou conjunto de operações efetuadas sobre Dados Pessoais, por meios automatizados (Brasil, 2018).

Na sequência, no que concerne aos dados pessoais sensíveis, estes possuem sua definição prevista no Art. 5º, inciso II [5] e estão relacionados com a característica da personalidade do indivíduo, ora titular, quais sejam informações sobre raça, religião, etnia, vida sexual ou práticas ou orientação sexual, informações médicas ou de saúde, informações genéticas ou biométricas, modelos biométricos, crenças políticas ou filosóficas, partido político ou filiação sindical, informações de verificações de histórico ou dados judiciais tais como antecedentes criminais ou informações sobre outros processos judiciais ou administrativos (Brasil, 2018).

No que se refere aos agentes de tratamento de dados pessoais, estes possuem papel institucional e relevante ao tomarem decisões acerca da destinação dos dados, uma vez que a capacidade de decisão e realização de atividades é da instituição e não de funcionário ou empregado com destinação para tanto, e com isso, existem dois importantes agentes na relação, o controlador e o operador. Corroborando com esse entendimento, vejamos:

> Importante pontuar que tanto o controlador quanto o operador são as figuras que têm o papel institucional, quando tomam decisões, no caso do controlador, ou realizam atividades sob ordem e comando, no caso do operador, e não os colaboradores, servidores ou trabalhadores de tais pessoas naturais ou jurídicas.
>
> Isso quer dizer que o papel de controlador e de operador sempre estará vinculado a esta figura institucional, e não poderá ser apontado a um empregado específico da empresa, pois a capacidade de decisão e realização de atividades é sempre da instituição e não do funcionário. (Pinheiro, 2021, p. 16).

Nesse contexto, o Art. 5º, inciso VI[6] conceitua quem é o controlador, o qual pode tratar-se de pessoa natural ou jurídica de direito público ou privado, competindo a este as decisões quanto ao tratamento dos dados pessoais (Brasil, 2018). Com isso, cabe ao controlador recepcionar os dados pessoais dos titulares sempre em conformidade com o consentimento do indivíduo.

---

[5] Art. 5º Para os fins desta Lei, considera-se: 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).

[6] Art. 5º Para os fins desta Lei, considera-se: VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. (Brasil, 2018).

Quanto ao operador, a sua definição está estabelecida no Art. 5º, inciso VII[7], pelo qual realizará o tratamento e toda a operacionalização dos dados pessoais em nome do controlador, cabendo ao operador seguir as instruções recebidas da controlador em relação ao tratamento dos dados pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, devendo garantir a licitude e idoneidade, sob pena de arcar com as perdas e danos que eventualmente possa causar, sem prejuízo das demais sanções aplicáveis, em especial do art. 52, da Lei 13.709/2018 (Brasil, 2018). Segundo Garcia:

> No caso de descumprimento da lei, cabe indenização e multa, sendo que Operador e Controlador são solidários entre si, ou seja, é possível cobrar de um, de outro ou de ambos. Da mesma forma, há a possibilidade de regresso, ou seja, aquele que pagar a indenização para o Titular pode cobrar do outro. Além disso, os Titulares podem processar de forma coletiva tanto o Operador quanto o Controlador (Garcia et al., 2020, p. 22).

Na sequência, ressalta-se que a LGPD predispõe e limita em seu Art. 5º, inciso IX[8] a atribuição de agentes de tratamento apenas ao controlador e ao operador, contudo é imperioso salientar que caberá ao controlador e ao operador indicarem um encarregado para atuar como canal de comunicação entre o controlador, os titulares e, ainda, manterá a comunicação com a autoridade nacional, sendo este denominado de Data Protection Officer (DPO), tratando-se de uma pessoa física ou jurídica, interno ou externo, individual ou trabalhando de forma conjunta e colegiada com um comitê (Brasil, 2018).

> Portanto, é possível nomear um colaborador interno para ocupar essa posição, assim como é possível contratar uma empresa que preste este tipo de serviço, conhecido por "DPO as a servisse".
>
> A LGPD previu que tanto o controlador como o operador devem indicar o encarregado, não fazendo qualquer distinção de porte de empresa, quantidade de funcionários, volume de tratamento de dados nem outras características específicas do perfil da base de dados pessoais (se envolve dados sensíveis) como ocorre no GDPR, mas pode haver alteração futura deste requisito por regulamentação específica da ANPD. (Pinheiro, 2021, p. 16).

Por conseguinte, é requisito necessário para o tratamento, o consentimento do titular dos dados, o qual anuirá e consentirá por meio da expressão de vontade em concordar ou não com o armazenamento, coleta, processamento, e demais operações relativas dados pessoais,

---

[7] Art. 5º Para os fins desta Lei, considera-se: VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (Brasil, 2018).

[8] Art. 5º Para os fins desta Lei, considera-se: IX - agentes de tratamento: o controlador e o operador. (Brasil, 2018).

devendo o indivíduo titular ser informado acerca de toda a destinação e finalidade para o qual os seus dados serão utilizados.

> Deverá o consentimento ser fornecido por escrito, com cláusula destacada das demais, ou por outro meio que demonstre a manifestação da vontade do titular. Nesse sentido, cabe ao controlador o ônus da prova de que o consentimento foi obtido de maneira livre e informada. Essa medida é essencial para resguardar a legitimidade da expressão de vontade não apenas formal, mas também material (Fernandes; Carvalho, 2018, p. 359).

Por fim, é imperioso ressaltar que as informações devem ser claras e objetivas, bem como, de fácil entendimento, não devendo haver conteúdo abusivo ou enganoso, de forma que não reste qualquer dúvida ao titular acerca do que esteja consentido.

2.4 A Proteção de Dados pessoais como um direito fundamental e a promulgação da Emenda Constitucional 115/2022

Antes de tudo, torna-se pertinente ressaltar e nos aprofundarmos sobre as disposições do direito constitucional em face ao tratamento de dados pessoais. Anterior à promulgação da Emenda Constitucional 115/2022, a qual será elucidada posteriormente, a Constituição Federal de 1988 não previa expressamente e diretamente qual a segurança jurídica seria dada aos dados pessoais, contudo, não se pode esquecer que o Art. 5º dispõe expressamente sobre o caráter inviolável da intimidade dos sujeitos, correlacionando, assim, com a proteção e inviolabilidade dos dados pessoais de cada consumidor. Revigorando com esse entendimento, Tomasevicius Filho (2021, p. 173- 174) aponta:

> Antes de analisar-se a LGPD, faz-se necessário retomar um debate sobre o direito constitucional sobre os dados pessoais. De fato, não há uma previsão constitucional direta que trate da proteção de dados. Contudo, não se deve olvidar que a Constituição Federal, ao optar por positivar um "conceito materialmente aberto de direitos fundamentais consagrado pelo art. 5º, §2º da CF aponta para a existência de direitos fundamentais positivados em outras partes do texto constitucional e até em tratados internacionais, bem assim para a previsão expressa da possibilidade de se reconhecer direitos fundamentais não-escritos". Há, de forma expressa, conforme nos lembra Afonso da Silva, a declaração sobre o caráter inviolável da intimidade dos sujeitos, da sua vida privada, da sua honra e da sua imagem, como previsto no art. 5º, X. Nas palavras do autor, o constituinte "erigiu, expressamente, esses valores humanos à condição de direito individual, mas não o fez constar do caput do artigo. Por isto, estamos considerando-o um direito conexo ao da vida. Assim, ele figura no caput como reflexo ou manifestação deste".

Assim como é possível e necessário dimensionarmos os demais direitos fundamentais em geral previstos na Constituição Federal de 1988, é imperioso evidenciarmos

que a Proteção de Dados Pessoais se tornou uma garantia fundamental, de forma a assegurar a inviolabilidade da privacidade de cada indivíduo titular de um dado, seja ele pessoal ou sensível.

Fazendo uma análise sobre o assunto em comento, é possível delinearmos que foi promulgada a Emenda Constitucional de nº 115, de fevereiro de 2022, de maneira a alterar a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Conforme vejamos abaixo:

> Art. 1º. O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX: "Art. 5º - LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".
>
> Art. 2º. O caput do art. 21 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXVI: "Art. 21 – XXVI - organizar e fiscalizar a proteção e o tratamento de dados pessoais, nos termos da lei.".
>
> Art. 3º. O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX: "Art. 22 – XXX - proteção e tratamento de dados pessoais". (Brasil, 2022).

Nesse sentido, a promulgação da Emenda supramencionada permitiu uma maior segurança jurídica na aplicação da Lei Geral de Proteção de Dados, garantindo ao titular dos dados uma proteção concreta e constitucional perante a privacidade das suas informações.

3 A NORMATIVA EUROPEIA DE PROTEÇÃO DE DADOS E AS REPERCUSSÕES DAS DISCUSSÕES E MARCOS LEGAIS NO DIREITO BRASILEIRO

O tema proteção de dados pessoais vem sendo bastante discutido não somente no Brasil, mas em todo o mundo, ganhando uma maior relevância nos últimos anos devido a ampla utilização dessas informações que são coletadas por empresas, que vem sendo usadas, e em algumas vezes até de forma indevida e sem um correto controle, de modo que as informações são vazadas gerando prejuízos ao seu titular.

Visando proteger os dados do titular, deu-se início a criação de uma ferramenta para tal fim, com o intuito de regulamentar essa prática e com foco na proteção do consumidor. Diante dessa proposta várias ações foram sendo desenvolvidas em vários países. Corroborando com essa temática, Doneda (2006, p. 239) explica que:

> O início do debate público acerca da necessidade de proteção de dados pessoais está relacionado à tentativa de alguns governos, nas décadas de 1960 e 1970, de efetuarem a centralização de diversos bancos de dados automatizados em um gigantesco banco de dados nacional, o que ensejou a reação da população e, consequentemente, influenciou a aprovação da primeira geração das normas de proteção de dados pessoais, tanto nos EUA como na Europa.

O autor supracitado menciona como exemplo o caso dos Estados Unidos, onde o Nacional Data Center, apresentado em 1965 por *Bureau of Budget*, que devido a reação da sociedade, jamais foi colocado em prática nos moldes propostos. Porém, foram percebidas algumas vantagens, tais como:

> [...] possibilidade de se extraírem estatísticas de forma precisa e ágil, de se rastrearem e corrigirem inúmeros dados equivocados dos cidadãos e de utilizarem com grande eficiência os dados pessoais para as inúmeras atividades estatais, facilitando a tomada de decisões e o planejamento de ações (Garfinkel, 2000, p. 13).

A ideia de que o centro deveria ter acesso aos dados dos cidadãos, como registros de nascimento, escolaridade, impostos dentre outros foram sendo evidenciados com a evolução do projeto. Tal fato originou diversos debates nos meios de comunicação, assim como originou várias audiências no congresso americano, que culminaram em um entendimento unânime a respeito dos danos que poderiam ser causados com esse tipo de centralização, principalmente devido ao poder conferido ao Estado.

Nessa seara destaca-se também casos semelhantes que ocorreram na Europa, como o projeto *Système Automatisé pour lês Fichiers Administratifs et lê Répertoire de Individus*

(SAFARI) apresentado na França pelo Instituto Nacional de Estatística em 1970. Ao analisar as leis que tratam essa temática nesses países, percebe-se algumas semelhanças, assim como algumas diferenças legislativas entre os países da Europa a respeito do tema, além das particularidades nos diversos estágios de evolução. Sob a perspectiva histórica da legislação europeia, a primeira geração de normas visando proteger os dados pessoais surgiu na década de 1970, as quais podem ser citadas:

> [...] as leis do Estado alemão de Hesse (1970), a Lei de Dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974) e a Lei Federal de Proteção de Dados da Alemanha (1977). Todas essas normas podem ser consideradas de primeira geração pela sua estrutura e linguagem (Bennett, 1992, p. 221).

Segundo o autor supracitado, o surgimento dessas normas foi impulsionado principalmente pelo contexto generalizado do Estado Social. Tal fato aconteceu pois, fazia-se necessário um planejamento sofisticado para o financiamento de sua burocracia. Destaca-se que, para esse tipo de planejamento ser alcançado, fazia-se necessário fazer a coleta e processamento dos dados pessoais.

No entanto, a sociedade em geral não aprovou as investidas do governo em fazer uso dos recursos tecnológicos para ampliar a coleta e o processamento dos dados, reagindo fortemente contra. Segundo Doneda (2006), o projeto não evoluiu, pois não foi bem aceito na esfera pública, pois considerou-se a violação da privacidade dos cidadãos e temiam que houvesse o controle absoluto de uma burocracia automatizada e desumanizada. Complementando esse contexto, Bennett (1992, p. 223) menciona que:

> Sob essa ótica, é possível perceber que grande parte das normas de proteção de dados pessoais da década de 1970 tem uma perspectiva funcional e busca controlar os bancos de dados de forma ex ante, condicionando o seu funcionamento à licença prévia ou ao registro nos órgãos competentes.

Com isso, o plano de centralizar os dados pessoais em um só banco de dado não foi concretizado. Devido a negativa do projeto, novas debates foram gerados fazendo surgir a necessidade de alterar a legislação, abrindo assim espaço para segunda geração de normas com foco na proteção de dados pessoais. Então, em 1978 foi aprovada a lei francesa de proteção de dados pessoais. Sobre essa temática, Sarmento e Galdino (2014, p. 348) destaca um outro tipo de temor, ou seja:

> O temor por um banco de dados único e centralizado foi substituído pelo temor da existência de milhares de bancos de dados espalhados pelo mundo, conectados em rede. Nesse contexto, entendeu-se que o melhor seria que os cidadãos lutassem pela preservação de sua privacidade a partir de direitos fortes, inclusive, protegidos constitucionalmente, em alguns casos. São exemplos de normas da segunda geração as leis da Áustria, da Franca, da Dinamarca e da Noruega.

Na segunda geração, os autores supracitados elucidam que a principal característica se refere à possibilidade do indivíduo participar do processo de coleta e processamentos de dados, a partir do seu consentimento para tal finalidade, dando assim ao cidadão o poder de terceiros interferir na sua privacidade informacional. Contudo destaca-se uma controvérsia existente na segunda geração das leis, a qual está relacionada à efetividade do consentimento do titular dos dados, ou seja:

> Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca do cadastro de suas informações pessoais (Mandarino Junior, 2010, p. 299).

De acordo com o autor supracitado, esse impasse gera questionamento sobre a proteção dos dados pessoais e a privacidade do titular dos dados. Diante dessa controvérsia surge então a terceira geração das normas de proteção dos dados pessoais, que tem como marco inicial a decisão de 1983 do Tribunal Constitucional da Alemanha que declarou inconstitucional a Lei do Censo, que obrigava o titular a divulgar seus dados sem assegurar a proteção dos mesmos.

Fazendo um comparativo da segunda com a terceira geração dos normativos de proteção dos dados pessoais, percebe-se que estes se referem a participação do titular dos dados no processamento destes, como um envolvimento contínuo, abrangendo a coleta, armazenamento e tratamento, e não limitando-se a opção tudo ou nada. Martins (2005, p. 233) cita algumas leis que marcaram a terceira geração, são elas: “as leis dos Estados alemães após a decisão do Tribunal Constitucional, a emenda à lei federal de proteção de dados pessoais alemã de 1990, a emenda da lei da Áustria de 1986, a alteração da lei da Noruega e a previsão constitucional da proteção de dados pessoais da Holanda”.

No entanto, na prática, assim como na segunda geração os titulares dos dados não estavam dispostos a arcar com os custos monetários elevados e nem os sociais para exercer seus

direitos, consequentemente, não estavam dispostos a se privar do acesso a bens e serviços ou ainda, a benefícios.

Surge então a quarta geração de normas que tem como propósito resolver as lacunas até então existentes, ratificando as normas de controle relativas aos dados pessoais tão importantes para a sociedade. Nessa geração, alguns dados relacionados a etnia, opinião religiosa e política, assim como opção sexual foram então proibidos de total ou parcial a partir da decisão do titular. Assim, algumas medidas foram estabelecidas, como:

> A proibição total do tratamento desses dados deu-se nas legislações da Noruega, da Finlândia, da Dinamarca, da França e da Grã-Bretanha. Já as legislações da Suíça e da Alemanha, assim como a Diretiva Europeia sobre proteção de dados pessoais de 1995, restringem o processamento de dados sensíveis, sem determinar, no entanto, a sua proibição total (Martins, 2005, p. 278).

Sobre a quarta geração o autor supracitado menciona também que se refere ao fato de que diversos países seguem suas diretrizes e estas se complementam com normas setoriais, com o intuito de ampliar a proteção do cidadão nos diversos setores em que é possível tratar seus dados pessoais.

3.1 O pioneirismo europeu na proteção de dados e a sua influência no contexto brasileiro moderno

A privacidade, a proteção de dados e os demais assuntos correlacionados não são novos no Brasil. No entanto, as discussões sobre a proteção e a privacidade de dados pessoais, em razão do surgimento de problemas decorrentes da era da informação em que vivemos e que percorrem, atualmente, o mercado e a academia, principalmente, são resultado de uma longa construção que culminou, no Brasil, por exemplo, na aprovação da Lei de nº 13.709, de 14 de agosto de 2018, ou simplesmente LGPD.

Nesse sentido, é importante destacar que com o crescimento e o desenvolvimento do cenário tecnológico diversos acontecimentos a nível mundial trouxeram à tona a necessidade de se discutir a questão. Tal fato aconteceu por causa da necessidade de as informações pessoais precisarem ser tratadas com um cuidado maior durante o armazenamento em meios eletrônicos, citando como exemplo, o Ato de Proteção de Dados de Hesse, uma lei que à época tratou da coleta e do tratamento de dados de indivíduos, mesmo não sendo de forma objetiva e segmentada (Mandarino Junior, 2010). À título de informação basal, vale aprofundar que o Ato de Proteção de Dados de Hesse, também conhecido como Lei de Proteção de Dados de Hesse

(*Hessisches Datenschutzgesetz*), é amplamente reconhecida como a primeira lei de proteção de dados do mundo, aprovada em 1970 pelo parlamento do estado alemão de Hesse. Este ato foi um marco na proteção da privacidade e dos dados pessoais, estabelecendo a base para futuras legislações de proteção de dados em outros países.

Ainda nesse sentido outros marcos legais como o Ato de Dados Sueco ou os próprios movimentos em diversas nações europeias que trabalharam ditames na tentativa de regular as ações de indivíduos ou coletividade no âmbito virtual, no que tange os dados desses de uma forma geral, além de tentar preservar ou garantir direitos – pode-se ilustrar isso com o exemplo da Áustria, Espanha e Portugal, da Espanha que consideraram a privacidade na sua Constituição como sendo um direito fundamental (Limberger, 2016).

Embora essas iniciativas no campo legislativo fossem à época muito importantes, eram genéricas, e assim denotavam a necessidade de uma discussão cada vez mais aprofundada e objetiva sobre o assunto. Por esse prisma, na década de 1980 foi aprovada pelo Conselho da Europa a Convenção 108 que tinha como fim, na prática, proteger as pessoas do tratamento automatizado de seus dados que possuíam um caráter mais pessoal.

Ademais, com o eminente crescimento do cenário da tecnologia, as normas relacionadas à proteção de dados começaram a alcançar mais espaço e começaram a tomar formas mais modernas como as que conhecemos hoje.

Ao longo dos anos, com os avanços tecnológico em todos os países, as leis voltadas para a proteção de dados pessoais passaram a ter uma importância maior, passando a ter uma similaridade com as leis atualmente vigentes. Um grande marco na Proteção de Dados pessoais aconteceu com a promulgação da Diretiva 95/46/CE do Parlamento Europeu e do Conselho, em 1995, pois tratava de dados e direitos dos titulares dos dados no mundo todo fazendo com que sejam tratados sob a mesma legislação (Pereira, 2016). A Diretiva, que posteriormente foi substituída pelo Regulamento Geral sobre a Proteção de Dados (RGPD), em 2018, estabeleceu as regras básicas para a proteção de dados pessoais na União Europeia (UE). Esta diretiva visava garantir a liberdade de circulação de dados entre os estados membros, enquanto protegia os direitos e liberdades fundamentais das pessoas singulares.

3.2 As repercussões do regulamento (UE) nº 2016/679 no direito brasileiro

Sobre a Diretiva 95/46/CE Nakata (2019, p. 1) explica que esta "vigorou até maio de 2018, e foi substituída pela nova lei de Proteção de Dados da União Europeia, o Regulamento

nº 2016/679, de 27 abril de 2016, popularmente conhecido como General Data Protection Regulation (GDPR)".

A GDPR é uma legislação é conhecida por ser muito completa, que mudou o tratamento de dados principalmente por propor aos direitos dos usuários uma ampliação de direitos, além de estabelecer uma responsabilidade maior as empresas responsáveis realizarem a coleta e tratamento dos dados. Esse procedimento passou a ser aplicado em todos os países da Europa assim como muitos outros que tem contato com o mercado europeu, ao redor de todo o mundo.

Segundo Nakata (2019) a proposta da lei é que sejam inclusos não somente os dados de pessoais nascidos nos países da União Europeia, mas também nos demais. Considerando ainda o texto proposto pela GDPR, fica evidente que países que apresentam tais "níveis de adequação" podem com mais facilidade realizar a transferência dos dados para outros países, desde que estes estejam também sob a jurisdição da GDPR, evidenciando assim, a influência desta lei. Sobre essa temática, o autor então afirma que:

> Países da América do Sul como: Argentina, Chile, Colômbia, Peru, Uruguai, Paraguai e Guiana Francesa foram pioneiros no continente em elaborar suas leis de proteção de dados, no Brasil isso só foi ocorrer com a aprovação da Lei nº 13.709, de 14 de agosto de 2018, também conhecida como LGPD (Nakata, 2019, p. 1).

Observa-se assim que com a proposta de implantar lei para proteger os dados de pessoas ganhando uma relevância cada vez mais em todo o mundo entre os anos de 1970 a 2018, principalmente entre os países que fazem parte da Europa e do continente sul-americano, foi possível perceber de forma mais evidente o impacto tecnológico na esfera global.

3.3 Construção e implementos da Lei Geral de Proteção de Dados no direito brasileiro

Sobre a proteção de dados foi sendo construída ao longo dos anos no Brasil uma agenda de debates e discussões devido a evolução da tecnologia, sendo redigido pelo Ministério da Justiça um Anteprojeto de Lei de Proteção de Dados (APLPD), que tinha como propósito disponibilizar uma consulta com a opinião pública. Tal proposta acabou criando um blog que tratava especificamente sobre proteção de dados, sendo este disponibilizado no site "culturadigital.br" para Consulta Pública.

Tal fato aconteceu depois de quatro meses de duração e uma grande repercussão em diferentes nichos da sociedade, principalmente pelo Marco Civil da Internet ainda ser um tema

bastante discutido na época, e ambos eram bastante associados, inclusive com uma denominação parecida, o chamado “Marco Legal da Proteção de Dados”, assim foi dada a largada no Brasil para uma nova era, com uma maior atenção aos Dados Pessoais.

Pereira (2016) menciona então que a construção de marco durou cerca de 8 anos tendo alguns estágios de consulta. A primeira delas ocorreu na Câmara dos Deputados quando o Deputado Milton Monti, em 13 de junho de 2012, inspirado na própria consulta pública realizada pelo Ministério da Justiça apresentou o Projeto de Lei nº 4.060 de 2012 (PL nº 4060/12) que se refere ao tratamento de dados pessoais. No entanto, por não ter instigado o interesse como pretendia, o referido projeto foi protocolado na Câmara e somente em 2013 voltou a ser discutido.

Passados dois anos, o tema que não tinha avançado significativamente só retornou em pauta em 2015 quando ocorreu novamente uma promoção feita pelo Ministério da Justiça. Houve então a segunda consulta pública do referido anteprojeto, que seguiu a mesma premissa da primeira, ou seja, os dados para consulta foram disponibilizados no site “culturadigital.br”.

Nessa fase houve uma maior contribuição da sociedade com sugestões de alteração do texto, assim, foi protocolado o Projeto de Lei que recebeu o número 5276/16 (PL nº 5276/16), que avançou de forma mais acelerada, por possuir um texto mais completo. Assim, tanto a Câmara como o Senado, no dia 25 de maio de 2018, decidiram devido ao impulsionamento dado com a promulgação da GDPR que passou a vigorar em 25 de maio de 2018 se unir em um único propósito que foi de defender o texto do Projeto de Lei nº 5.276/16, considerado melhor para substituir o Projeto de Lei nº 4.060/12, o que demonstra o grande interesse e contribuição da população na sua criação.

Com essa união da Câmara e Senado, o Brasil, depois da primeira lei de proteção de dados no mundo vigorar há 48 anos, passou a ter a sua própria lei de proteção de dados. Com isso, o país passa a ter então uma expectativa mais concreta proteção maior de direitos e garantias para os cidadãos, que se fundamentou a partir da aprovação da Lei Geral de Proteção de Dadas cujas garantias estão protegidas pela Constituição Federal de 1988, abrangendo inclusive meio online e offline, por tratar da individualidade e privacidade dos cidadãos, também resguardando o direitos individuais, desenvolvendo a inovação com base nas regras que foram definidas de forma transparente e clara.

4 INTERFACE DA LEI GERAL DE PROTEÇÃO DE DADOS: O ESCOPO DA CONSTRUÇÃO DO DIREITO À PROTEÇÃO DE DADOS

A ideia de resguardar os direitos a intimidade, privacidade e a proteção de dados surgiu originalmente com criação do Código Penal em 1940, quando tratou da inviolabilidade da residência, apesar de não dispor de maneira direta sobre dados pessoais, ao proteger a residência tratou sobre privacidade. A Constituição de 1988 traz em seu texto, nos artigos 5º, inciso X, a inviolabilidade da intimidade e da vida privada, mostrando também a importância da proteção a individualidade.

A Lei nº 8.078, de 11 de setembro de 1990, Código de Defesa do Consumidor foi primeira lei brasileira que tratou especificamente da proteção de dados e direitos relativos a este. No artigo 43 da referida lei, por exemplo, trata de expor que o consumidor tem direito de ter acesso e corrigir informações referentes a si. O Código de Defesa do Consumidor é um grande influenciador da LGPD, por apresentar princípios semelhantes, como o princípio da finalidade e necessidade, e ser considerado por alguns uma legislação em favor do consumidor da era digital.

A LGPD não pretende substituir outras legislações, mas para apresentar e reorganizar regras e princípios gerais para que estas possam cumprir de uma maneira mais benéfica, especifica e eficaz os titulares de dados pessoais, podendo ser vista como uma diretiva geral.

4.1 Entendendo as bases legais da normativa brasileira

Para buscar o melhor entendimento em sociedade, a LGPD traz a definições importantes sobre “informação relacionada à pessoa natural identificada ou inidentificável”, com intuito de expor que qualquer informação, seja ela apresentada de forma separada ou associada a outras, pode identificar diretamente uma pessoa natural, essa forma de definição também busca aumentar o objetivo de aplicação da lei.

Os dados pessoais sensíveis é uma categoria muito importante trazida pela legislação, nela são indicadas as origens raciais ou étnica, opinião política, convicção religiosa, filiação a sindicato ou a disposição no âmbito político, fisiológico ou religioso, vida sexual, dado genético ou biométrico, dado referente a saúde, quando vincula a uma pessoa natural. Fica claro que essas informações podem gerar aos seus titulares algum tipo de descriminação e por

isso esses dados devem ser objeto de mais restritivas e padrões de segurança mais elevado, daí vem a nomenclatura “dados sensíveis” (Santos, 2012).

Outra importante categoria explanada pela lei refere-se aos dados anonimizados, se referindo ao “que não possa ser identificado, utilizando-se meios técnicos razoáveis e disponíveis na ocasião de seu tratamento”, isso quer dizer que, esses dados não ficariam sujeitos as normatizações da lei se não pudessem ser identificados (NAKATA, 2019, p. 1).

Essas categorias de dados pessoais, para que possam ser tratados respeitam princípios gerais para que sejam considerados tratamentos legítimos e lícitos. Assim, a lei traz 10 (dez) hipóteses que permite de forma legal o tratamento de dados. O consentimento do titular é umas das hipóteses, esse consentimento deve ser demonstrado de forma escrita ou qualquer outro meio que manifeste a vontade do titular, tendo o direito inclusive de forma gratuita e facilitada, de anular o seu consentimento. Nesse contexto, destacam-se um conjunto de bases legais:

> (i) o consentimento do titular; (ii) o cumprimento de obrigação legal ou regulatória pelo controlador; (iii) a execução de políticas públicas; (iv) a realização de estudos por órgãos de pesquisa; (v) a execução de contrato de qual seja parte o titular; (vi) o exercício regular de direito em processo judicial, administrativo ou arbitral; (vii) a proteção da vida; (viii) a tutela da saúde; (ix) o legítimo interesse; e, por fim, (x) a proteção ao crédito, além disso, é importante destacar o significado de controlador, aquele que trata e fica responsável pelos dados, e seu legitimo interesse, onde poderá fundamentar o tratamento dos dados para finalidades legítimas, sempre observando em casos concretos, independente do consentimento do titular, uma vez que todas as bases legais são independentes entre si e nenhuma sobrepondo a outra (Brasil, 2018).

No que se refere aos dados pessoais sensíveis em relação aos dados pessoais comuns, estes dispõem normas mais rígidas, podendo citar como exemplo, a especificação e destaque da finalidade de tratamento descritas, existindo exceções, no caso de ser imperativo para a realização das atividades descritas em lei. Ademais, é importante expor também, a categoria dos dados pessoais de criança, cuja idade seja de até 12 anos. Deverá ser realizado pelos seus pais ou representante legal, o consentimento para tratamento específico.

A LGPD traz uma diferenciação muito importante de anonimização e pseudoanonimização, e esse ponto é importante por destacar bem que “os dados anonimizados são aqueles que não podem identificar o titular utilizando meios técnicos razoáveis e disponíveis na época de seu tratamento, sendo retirados, portanto, da legislação, pois não caracteriza dados pessoais” (Pezzi, 2019, p. 1). Os pseudonimizados são aqueles dados que impossibilita a identificação ou associação de um indivíduo, que segundo Nakata (2019, p. 1):

> [...] esses dados só podem ser utilizados na realização de pesquisas referentes a saúde pública, conforme artigo 13 da legislação. Portanto, a lei não obriga a anonimização,

> mas explica que quando possível para isso seja feito, isso significa que se existe uma empresa, que em seus serviços trabalha com bases em CPF, e precisa desse identificador para poder gerar um target, ou realizar enriquecimento de dados, por exemplo, ela não poderá anonimizar a sua base de dados, porque isso impossibilita os seus serviços, e assim poderá tão somente, pseudonimizar e criptografar os dados, a fim de mitigar riscos associados a possíveis vazamentos.

Para maior eficácia da Lei Geral de Proteção de Dados é importante definir o uso compartilhado de dados, pois com sua definição, as pessoas terão mais consciência ao propagarem seus dados, a legislação define esse compartilhamento como:

> [...] comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, uma ou mais modalidades de tratamento permitidos por esses entes públicos, ou entre entes privados, para esse compartilhamento dos dados pessoais é necessário uma base legal sólida e adequada a esse contexto (Brasil, 2018).

É importante o controlador ter de forma atenta o monitoramento dos dados pessoais que transfere, pois qualquer cidadão titular de seus dados tem o direito de saber com quem e para quais finalidades seus dados foram utilizados para compartilhamento, inclusive, o direito de correção, eliminação, anonimização ou bloqueio de dados.

Vale destacar também, que o Poder Público tem uma maior liberdade no que tange ao compartilhamento de dados entre os entes e órgãos da Administração Pública, essa liberdade só pode ser aproveitada mediante previsão legal específica, com a apresentação de suas finalidades, isso porque tem de ser respeitados princípios da legislação como o da finalidade e legalidade, esses dados, inclusive, podem ser de dados sensíveis, estruturação de dados pessoais para uso compartilhado e outros. Alguns exemplos dessa maior liberdade, acontece, nos casos de aplicação da Lei de Lavagem de Dinheiro, Lei de Combate às Organizações Criminosas e Lei de Acesso à Informação.

Por fim, além das regras já dispostas na LGPD, a Autoridade Nacional de Proteção de Dados é uma personagem fundamental para o melhor funcionamento da legislação, garantindo sua vigência e eficácia nessa era digital, podendo organizar, monitorar e estabelecer normas complementares sobre o uso compartilhado de dados pessoais. A Autoridade Nacional de Proteção de Dados, inclusive, tem como função fiscalizar o cumprimento das disposições presentes na LGPD, bem como aplicar as sanções cabíveis no caso de infração de uma ou mais delas.

4.2 Origem da autoridade nacional de proteção de dados e as sanções que implementam e fortalecem a proteção de dados

A Autoridade Nacional de Proteção de Dados (ANPD), é órgão federal de suma importância para o ambiente de proteção de dados nacional tendo em vista a sua colaboração na elaboração de normas e em fiscalizar os procedimentos sobre a proteção e tratamento de dados pessoais.

Com isso, a legislação editada no ano de 2018 pelo então presidente Michel Temer, a Medida Provisória 869 modificou a LGPD, (Lei nº 13.709, de 2018), norma que regulamentou a forma como as organizações (empresas, bancos, órgãos públicos e outras empresas) utilizam os dados pessoais.

A Medida Provisória foi regularmente aprovada em maio daquele ano pela Câmara e pelo Senado, e saiu com diversas modificações em relação à redação original, isso ocorreu em 27 de dezembro de 2018, e o então Presidente Michel Temer publicou no Diário Oficial da União em 28 de dezembro de 2018, que, além de promover determinadas alterações no texto sancionado da LGPD criou a Agência Nacional de Proteção de Dados, órgão este que está na administração pública federal diretamente vinculado à Presidência da República.

A Medida Provisória nº 869/18 estipula que a Agência Nacional de Proteção de Dados será composta por seis departamentos: Conselho Diretor; Conselho Nacional de Proteção de Dados Pessoais e Privacidade; órgão de assessoramento jurídico e as unidades especializadas, que irão atuar de forma distribuída pelo país com a finalidade de pôr em pratica o que traz a legislação.

É importante destacar que, as sanções são sem dúvida alguma um dos principais instrumentos que a Agência Nacional de Proteção de Dados dispõe para exigir o cumprimento da legislação, que deve ser aplicada conforme parâmetro de gravidade, natureza das infrações, dos direitos pessoais afetados, a boa-fé do infrator, a vantagem auferida ou pretendida pelo infrator, a condição econômica do infrator, a reincidência, a extensão do dano, a cooperação do infrator, comprovação de utilização de mecanismo capazes de minimizar os danos, a adoção de políticas de boas práticas e governança e a pronta adoção de medidas corretivas.

A Agência Nacional de Proteção de Dados possui o poder, através de seu regulamento, escolher artifícios para a orientação do cálculo do valor-base das sanções administrativas referentes à LGPD, inclusive sendo objeto de consulta pública.

As sanções para as empresas que tratam dados, visam a melhor aplicação da LGPD e variam entre as mais brandas, como a advertência, onde a empresas devem adotar medidas

corretivas dentro de um prazo que será indicado, multas simples ou diárias de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, essa multa se limita a um valor no total de R$ 50.000.000,00 por infração, publicização que será após a comprovação da ocorrência e sua gravidade de vazamento de dados, bloqueio e eliminação de dados até sua regularização, no que se refere a infração, a empresa fica impedida de exercer suas atividades podendo causar até mesmo sua falência.

Vale ressaltar que a aplicação das sanções administrativas será feita num ambiente de proteção constitucional da ampla defesa e o contraditório, onde eventual irresignação se submeterá aos primados do devido processo legal. De forma que, à título exemplificativo, a ocorrência de qualquer incidente de segurança, o Agente Digital, caso opere como controlador, deverá notificar a Autoridade Nacional de Proteção de Dados, em tempo razoável.

5 OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS NAS RELAÇÕES CONSUMERISTAS E EMPRESARIAIS CONTEMPORÂNEAS

Com a evidente expansão tecnológica que vem acontecendo em consequência da globalização, as empresas para manter-se ativas e competitivas no mercado estão reinventando suas estratégias empresariais, investindo principalmente em Propaganda e Marketing. Pensando nisso, o acesso as informações pessoais dos consumidores passam a ser consideradas como maior chance de sucesso, isso porque, além de conseguir uma abordagem mais direta, passam a ter menor custos e um retorno econômico mais rápido.

Frente a esse cenário, é preciso que seja estabelecida uma relação transparente entre as empresas e os consumidores, de modo que os limites da privacidade, inviolabilidade da intimidade do cidadão nãos sejam ultrapassados. Para isso foi instituída a Lei nº 13.709/2018 que está em vigor desde 2020.

Assim, nessa seção pretendeu-se fazer uma explanação sobre a proteção de dados pessoais, fazendo uma reflexão do seu contexto nos dias atuais, assim como também sobre os reflexos da LGPD nas principais práticas empresariais, explanando sobre a LGPD em compliance, sobre os termos de uso de políticas de privacidade e finalizando com o tratamento da importância da figura do *Data Protection Officer* (DPO) nas empresas.

5.1 Proteção de dados e uma breve reflexão quanto a sua contemporaneidade

Inicialmente, é importante considerar que a LGPD não afeta somente grandes empresas que lidam de forma direta com o setor de tecnologia e serviços on-line, como Google e Facebook, mas afetam também qualquer pequena, média ou grande empresa que realize uma operação de coleta, uso, processamento e armazenamento de dados pessoais, ou seja:

> [...] a legislação abrange todos que compõem nossa sociedade de capitalismo, pois tanto protege quem consome quanto o que vende e fornece o produto ou serviço, portanto no âmbito de atividades de bancos, corretoras, seguradoras, clinicas médicas, hospitais, e-commerce, varejo, hotéis, companhias aéreas, agências de viagens, restaurantes, academias, entre muitas outras, podem estar sujeitas à aplicação da lei, ainda que tais atividades ocorram exclusivamente fora do ambiente digital (Pezzi, 2017, p. 254).

Ademais, com a entrada em vigor da LGPD, foi intenção do legislador alimentar e incrementar a própria economia, pelo motivo de que países que não dispõem de uma lei

protetiva de dados passam imagem negativa de segurança negocial e jurídica, e com isso se isolam no que tange ao comercio mundial, perdendo a oportunidade de firmar novos negócios.

É importante destacar que atualmente tudo isso tem implicação na forma de atuação das empresas, pois aquelas que não respeitarem de forma decidida a LGPD, ficará sem dúvida manchada no mercado, e com exposição relevante no caso de sanções e multas aplicadas, caindo de forma exponencial a credibilidade de uma empresa que negligencia o cuidado e tratamento de dados de seus clientes (Nakata, 2019).

Portanto é crucial que todas as empresa se adequem a legislação, pois sua indiligência pode ser gravemente prejudicial para sua imagem no mercado, como também, em caso de adequação, podem se tornar um fator de prestigio e admiração, sendo capaz de impulsionar aquela pessoa jurídica que fica conhecida por passar segurança ao consumidor no que tange a organização, respeito e proteção aos dados pessoais de seus clientes, respeitando de forma incisiva a legislação, assim, a lei pode proporcionar e impactar no mercado situações positivas e negativas para todas as empresas dos mais variados ramos.

5.2 Os reflexos da LGPD nas principais práticas empresariais

Nos últimos anos, a sociedade tem passado por uma mudança tecnológica muito grande, afetando todos os lados da vida humana. Mas esse progresso rápido muitas vezes esconde o fato de que a privacidade, um direito ganho com o tempo, tem sido questionada e mudada no campo legal.

Como evidenciado ao longo deste estudo, a técnica não só mudou os laços sociais e como a informação passa, mas também pediu da área jurídica um esforço para equilibrar novidade e cuidado com os direitos básicos. Assim, perceber a intimidação causada pelo volume de restrições impostos pela LGPD não precisa ser visto como um empecilho ao avanço, mas como uma necessidade importante para garantir que os benefícios do uso da tecnologia vão juntos com a proteção da honra e liberdade das pessoas.

Nessa seara destaca-se a preocupação com o tratamento de dados pessoais. Assim, para analisar os reflexos da LGPD nas principais práticas empresariais, na sequência, faz-se uma abordagem sobre LGPD em compliance, sobre os termos de uso de políticas de privacidade da função à prática e a respeito da importância da figura do *Data Protection Officer* (DPO) nas empresas.

5.2.1 LGPD em compliance

A LGPD trouxe diversos desafios para empresas e para as pessoas que compõem nossa sociedade, ambos devem se adequar às novas exigências legais, esse processo não será tarefa fácil, mas sem ele poderá gerar prejuízos imensuráveis, não só sob o ponto de vista financeiro, mas prejuízos éticos, morais, que podem ferir princípios como da intimidade, por exemplo, e o compliance que possui como principal foco e objetivo a prevenção e a reativação, gerando a redução de danos. Corroborando com essa temática, Oliveira, Zanetti e Lima (2019, p. 6) afirmam que:

> Inicialmente, o empresário que usa, coleta ou armazena dados de qualquer pessoa deve observar, além da boa-fé, os princípios trazidos pela Lei 13.709/2018, no art. 6º, para se manter em compliance. Tais princípios apresentam-se discriminados com sua aplicação prática, o que facilita a sua incorporação pelas políticas de proteção de dados.

Para os autores supracitados, tais princípios foram desenvolvidos a partir de mecanismos internacionais e transnacionais, considerando a privacidade com relação a proteção de dados pessoais, os quais estão sendo implantados na legislação e normatização brasileira. Segundo Nakata (2019) refere-se, portanto, dos princípios fundamentais do cidadão, os quais devem concretizados pelas empresas responsáveis por manipular os dados. Sobre o programa de integralidade, Veríssimo (2017, p. 91) explica que este possui algumas diretrizes que é tratado em três etapas:

> na primeira, correspondente ao conhecimento, ou seja, análise e valoração de riscos, definição de medidas de prevenção e a criação de uma estrutura de compliance; a segunda, implementação, ou seja, comunicação e detalhamento do programa, consistente em medidas organizacionais para criação de processos de compliance; a terceira, por fim, abrangendo a consolidação e aperfeiçoamento, estabelecendo um processo para apuração de violações, critério de sanções e avaliação continuada e aperfeiçoamento do programa.

Os riscos são reais e capazes de grandes prejuízos, eles são compostos de dois principais componentes: é o risco provável de ocorrência e a magnitude de perda, sendo que esta última consiste em “impacto”. Nesse contexto, a probabilidade de ocorrência pode ser representada pela frequência do evento danoso ou ameaça em determinado período de tempo. Quanto ao impacto, são direcionadas basicamente ao comprometimento de uma das propriedades básicas da segurança de informação: confidencialidade, integridade e disponibilidade (Vieira, 2017).

É importante expor, que existem alguns principais mecanismos para desenvolver as identidades da LGPD, o grupo de normas 27000, publicada pela *International Organization for Standardization* (ISO), é considerada uma das grandes ferramentas no que tange a proteção de dados.

Essa regulamentação normativa é importante pois é referencial de padrão internacional, já reconhecido e validado para proteção, segurança de informação. Entre outros aspectos, esse regulamento serve de parâmetro pois é guiado por um sistema de gestão que consegue precisamente avaliar riscos de segurança e proteção, possui procedimentos de controle, monitoramento de desempenho dos processos, servindo e atuando assim em sintonia, deixando mais eficaz com reforço dos programas de integridade que visam a proteção de dados e privacidade. Oliveira, Zanetti e Lima (2019, p. 12) seguindo essa temática, explicam que:

> Com isso, considerando que, para as atividades das instituições ou empresas, bem como evitar, detectar e tratar quaisquer desvios ou inconformidades que possam ocorrer, como riscos dos negócios e os preceitos que baseiam os programas de integridade, como: "prevenção, processamento de informações sensíveis, e treinamento de colaboradores, pode-se enquadrar a Lei Geral da Proteção de Dados, perfeitamente como um tema de compliance".

Isso significa que, para a LGPD se tornar mais eficaz e efetiva, deve manter e em compliance, nas instituições e empresas, que ainda devem observar outras questões práticas, a exemplo da elaboração de um adequado Termo de Uso e de Políticas de Privacidade, ferramenta importante para a consolidação e segurança do usuário.

5.2.2 Termos de uso de políticas de privacidade: da função à prática

Com a instituição da LGPD surge um novo meio de proteção no que se refere ao tratamento de dados em ambiente virtual, assim, a proteção da privacidade e intimidade deixa de ser meramente formal, inaugurando-se uma nova forma, que se impõe a essa tutela material.

Esse fato, se diz respeito, por mesmo no âmbito das relações digitais estabelecidas via internet, que interliga pessoas no mundo todo, já havia legislação própria para regular o tema da proteção de dados, ainda que de forma incompleta, considerando que a questão da proteção de dados até então era regida pela Lei nº 12.965/2014, conhecida como "Marco Civil da Internet", verificava-se abuso contumaz praticado por empresas na coleta, tratamento e exploração de dados pessoais. Corroborando com essa temática, Oliveira, Zanetti e Lima (2019, p. 13) aduz:

> A atenção e cuidado no tratamento de dados realizados fora do âmbito digital, então, não está sujeito a qualquer controle mínimo e eficaz, mesmo que haja outras normas dispostas em leis esparsas, como o Código de Defesa do Consumidor (CDC) e as leis do Cadastro Positivo (Lei nº 12.414/2011) e de Acesso à Informação (Lei nº 12.527/2011), sem olvidar da garantia fundamental à vida privada, assegurada no artigo 5º, X, da Constituição Federal.

A referida mudança no padrão, influencia diretamente nas atividades empresariais, podendo até ser referida como "Quarta Revolução Industrial", que se destaca por importantes fatores, como "a velocidade, amplitude, profundidade e impacto sistêmico" (Schwab, 2016), as relações sociais cada vez mais se desenvolvem digitalmente, pelo fato da tecnologia crescer cada vez mais por todo mundo, e a sociedade se adaptar as facilidades e benefícios trazidas por ela.

Grandes bancos de dados, atualmente, são mantidos em nuvens (*cloudcomputing*) e outras espécies de bancos de dados exclusivamente digitais, ganhando enorme destaque em atividades, como exemplo da *'Data Mining'* (mineração de dados) e o chamado *'Big Data'* (grande volume de dados). Sobre essa temática, Oliveira, Zanetti e Lima (2019, p. 13) explicam que:

> Este fenômeno se deve especialmente pela globalização do comércio digital, com isso gera-se, razão do amadurecimento nas últimas décadas da importância do tratamento de dados e da importância da informação como ativo importante para o mercado, se tornando mecanismo para a expansão de mercado, considerados, sobretudo, os aspectos da 'maleabilidade' e 'utilidade' da informação, que exponenciam sua influência sobre as tomadas de decisão e a vida cotidiana em geral. Esse fato, cria um efeito de crescente expansão de atividades empresariais ligadas à exploração de dados, sistematização da informação e formação de bancos de dados.

De acordo com os autores supracitados, as relações consumeristas e empresariais foram diretamente afetadas com essa nova forma de se relacionar. Uma dessas mudanças originou a multiplicação dos documentos conhecidos como "Política de Privacidade" e "Termos de Uso", cujo o principal propósito é administrar as relações dos usuários que visitam sites e serviços de internet. Nessa seara, estão inclusas as seguintes ações: "proteção dos usuários, ligadas ao tratamento de dados pessoais, desde a coleta, passando pelo armazenamento, até sua eliminação" (Schwab, 2016).

Veríssimo (2017), sobre esses termos menciona também que eles não detêm características democráticas, haja vista que ao acessar um site busca-se por algo, seja comprar algum produto, ou solicitar algum tipo de serviço. Assim, ao estabelecer uma relação com uma determinada empresa, fornecedora, não se tem o poder de debater ou discutir no texto, assim

como nos efeitos das cláusulas descritas nos referidos documentos, restando ao usuário apenas a opção de aceita-los nos moldes apresentados, e se não os aceitar, rejeita-os. Logo o acesso ao conteúdo, serviço ou produto é negado ou limitado. Assim, a empresa que possui o domínio da relação constituída via internet ou aplicativo tem o dever de informar àqueles que adentram em seus sites ao tratarem de dados pessoais, como já disposto nos Termos de Uso e Política de Privacidade.

Vale ressaltar, mesmo que os Termos de Uso e Política de Privacidade sejam uma ferramenta importante para a proteção da privacidade em sites e aplicativos, em espaços privados, os usuários não podem sujeitar-se a termos de uso abusivos, que delimitam de maneira irregular seus direitos garantidos na Constituição Federal.

Considerando que o uso da internet é ferramenta essencial, para o bom funcionamento, para prospecção de clientes e a manifestação explicita da função social desempenhada pela atividade empresarial, e que é importante destacar que as plataformas virtuais não são mais visadas apenas como um ambiente para o mero exercício de direitos disponíveis, mas como meio um viável de exercer diversas práticas empresariais, direitos sociais e individuais.

É importante lembrar que mesmo enquanto a proteção de dados pessoais já existisse sob o pálio do Marco Civil da Internet, a LGPD, no entanto, abrange de forma mais completa, com diretrizes estabelecidas naquela norma, impondo às empresas novos desafios para se adequar à legislação. Corroborando com essa temática, Oliveira, Zanetti e Lima (2019, p. 17) afirmam que:

> É importante observar, que as empresas, em geral, que oferecem seus serviços pela internet, para enquadra-se de acordo com a Lei Geral de Proteção de Dados, inevitavelmente terão que desfrutar de seus Termos de Uso e Política de Privacidade informações transparentes e claras aos seus usuários, isso implica na forma de tratamento que é disposto aos dados pessoais, respeitando firmemente os princípios inseridos no artigo 6º da legislação, especialmente quanto à finalidade (I), adequação (II), necessidade (III) e transparência (VI).

Complementando esse contexto, Doneda (2010, p. 84) afirma que "[...] para salvaguarda das informações pessoais, estas deverão ser submetidas através de uma política de privacidade clara e precisa e do recurso a outros meios que garantam que sua inscrição não se efetive sem o real conhecimento das suas consequências".

O princípio da transparência talvez seja o principal elemento dos Termos de Uso e Privacidade, pois nesta ferramenta é necessário mostrar para que e porque seus dados são

coletados, tratados e utilizados, buscando uma clareza por parte da pessoa jurídica com aquele ato de recolhimento necessário, zelando pela possível hipossuficiência do consumidor.

Com esses aspectos, vale fundamentar um comparativo importante entre os Termos de Uso e Políticas de Privacidade, que apontam características explícitas de contratos de adesão, por possuir uma natureza industrial a depender do fornecimento e da forma de serviço, característica própria, são documentos semelhantes a uma 'Carta de Intenções', onde nesse instrumento é estabelecido previamente todos interesses, direitos, obrigações e demais regras consideradas necessárias para reger essa relação superficial que será formada entre as partes, delimitado apenas ao acesso ao determinado site, aplicativo ou plataforma disposto pela empresa.

Como já exposto, existem algumas disposições importantes e possíveis de serem apresentados Termos de Uso e Políticas de Privacidade como direitos e deveres dos usuários e cliente, esses preceitos mostram o percurso para o bom uso e utilização de serviços como sites, plataformas e aplicativos, com relação formada entre as partes, à proteção de propriedade intelectual sobre conteúdos veiculados a elas, responsabilidade e limites de comprometimento.

Criando um paralelo com a LGPD, é importante destacar e apontar quais serão os dados importantes e necessários para aquela coleta em prol do seu tratamento. Essa coleta deve se limitar aos dados mínimos necessários para a finalidade buscada pela empresa ou a quem o dado tenha sido fornecido, ou seja:

> [...] especificando e apontando para qual finalidade do tratamento, por qual prazo os dados serão tratados e o de que forma será realizada a eliminação dos dados quando do alcance da finalidade proposta, ou do exaurimento do prazo previsto art. 15, I e II, da Lei Geral de Proteção de Dados e qual serão os meios disponíveis e possíveis para que o titular dos dados (art. 5º, V, LGPD) possa exercer o direito de livre acesso aos dados tratados (art. 9º) (Pezzi, 2017, p. 288).

Com o surgimento das práticas de políticas de privacidade, nasce o dever de informe de algumas informações ao titular dos dados pessoais, essas informações abrangem que o tratamento de seus dados apenas será realizado em razão de alguma das hipóteses legais e determinações judiciais, previstas nos incisos do artigo 7º, da LGPD.

Desta forma, destaca-se que a LGPD expressa dez hipóteses que serão possíveis o tratamento de dados pessoais, porém, estabelecer a necessidade da coleta, em si, de ligação entre os Termos de Uso e Políticas de Privacidade e algumas das hipóteses legais.

5.2.3 A importância da figura do *Data Protection Officer* (DPO) nas empresas

Ao ser redigido o texto que varia parte da LGPD, foram estabelecidas algumas obrigações, sendo que uma delas, determina a necessidade de implementar um controle de dados pessoais, tanto na esfera pública, como na privada, com a indicação de um *Data Protection Officer* (DPO), que poderia ser uma pessoa jurídica ou natural, que teria a responsabilidade em desenvolver ações para assegurar a proteção dos dados coletados e tratados, além de atuar como interlocutor da comunicação entre as autoridades nacionais, os titulares dos dados e o controlador (Pezzi, 2017).

Para uma maior clareza, no site da empresa responsável pela coleta e tratamento de dados, deverá constar de forma clara e objetiva a identificação do encarregado, assim como a forma de comunicação. A ideia é facilitar as requisições, assim como a comunicação dos usuários e das autoridades nacionais. Oliveira, Zanetti e Lima (2019, p. 23-24), sobre essa temática explicam:

> Inicialmente as atividades do encarregado consistirão em receber reclamações e requisições dos titulares de dados, interagir com autoridade nacional de proteção de dados, orientar os funcionários e prestadores de serviços a respeito de boas práticas, bem como adotar as providências necessárias de proteção dos dados tratados.

Os referidos autores destacam a importância do conhecimento do encarregado, para que este possa fazer o acompanhamento e interagir com todos os fluxos estabelecidos nos processos internos da empresa responsável por controlar os dados, auxiliando diretamente no desenvolvimento dos serviços e produtos. Além desses pontos, Marcondes (2017, p. 254 cita:

> [...] na elaboração de termos de consentimento, no processo de anonimização dos dados armazenados em bancos de dados, entre outros, de maneira que possa supervisionar todas as práticas de tratamento de dados, e certificar se estão em compliance com a Lei Geral de Proteção de Dados.

O autor supracitado destaca então a importância no tratamento dos dados, sendo primordial que o encarregado tenha autonomia em desempenhar as suas funções, e principalmente, seja imparcial nas suas ações dentre da empresa. Além disso é importante que este possa interferir nos processos internos, sugerindo quando necessário, mudanças e adequações dos processos, mesmo que afete economicamente a empresa, haja vista que a questão é o cumprimento das normas.

6 CONCLUSÃO

Ao iniciar o desenvolvimento do estudo foram estabelecidos alguns objetivos que deveriam ser alcançados ao longo do trabalho, para que o leitor compreendesse melhor o tema em estudo. Assim, sobre a normativa europeia de proteção de dados e as repercussões das discussões e marcos no direito brasileiro, concluiu-se que o tema vem sendo ao longo dos anos bastante debatido em nosso país, amadurecendo as ações com audiências públicas que visam proteger os dados pessoais que estão sendo expostos com mais frequência devido aos eventuais vazamentos dessas informações.

Continua-se a pesquisa com um apanhado geral sobre a normativa europeia de proteção de dados, especialmente quanto ao *General Data Protection Regulation* (GDPR), aprovado pela União Europeia e em vigor desde 2018, destacando seus princípios, obrigações e direitos conferidos aos titulares de dados. Destarte, conduziu-se ainda o estudo sobre a repercussão de tais discussões dentro do cenário nacional, tentando evidenciar a influência direta da GDPR na construção da Lei Geral de Proteção de Dados Pessoais (LGPD).

A respeito da interface da LGPD, pode-se dizer que esta lei foi instituída com o intuito de organizar, monitorar e estabelecer normas para o tratamento de dados pessoais por terceiros. Assim, com a promulgação da referida lei, o Brasil passou a fazer parte do rol dos países que visam realizar o tratamento adequado de dados, com foco na proteção da privacidade do titular dos dados pessoais.

Sobre os impactos da LGPD nas relações consumeristas e empresariais contemporâneas, concluiu-se que foram criados com a referida lei as figuras do controlador e do operador, que decidem quanto ao tratamento dos dados pessoais. É importante mencionar que estes devem ter autonomia para desempenhar suas funções dentro da empresa, agindo sempre de forma imparcial, e, quando necessário, sugerindo mudanças e adequações para que a empresa cumpra as normas estabelecidas na lei.

A respeito da temática abordada ao longo do estudo, destaca-se que a LGPD, buscou tratar uma série de obrigações com o propósito de garantir a segurança das informações pessoais, notificando o titular dos dados no caso de incidentes de segurança e nos casos de legítimo interesse. Dessa forma, com as normas trazidas na referida lei, o titular ganhou uma série de direitos, como, por exemplo, solicitar a empresa a correção dos dados incorretos, podendo inclusive cobrar pela correção exigida. Para isso, a Autoridade Nacional de Proteção de Dados (ANPD) é a responsável pela fiscalização.

Com a conclusão do estudo e ciente de que o trabalho alcançou a proposta inicialmente estabelecida, mas que devido a possibilidade de analisar o tema em outras vertentes, deixa-se como sugestão para pesquisas futuras a elaboração de um instrumento de coleta para aplicar junto as empresas para saber a percepção destas sobre as medidas propostas com a promulgação da referida lei, podendo ser analisada também a percepção do público geral sobre a proteção dos dados pessoais.

REFERÊNCIAS

BENNETT, Colin. **Regulating Privacy**: data protection and public policy in Europe and the United States. Cornell University Press, 1992.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 12 out.2024.

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: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 12 out.2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). DOU Seção 1 - Edição Extra - 15/8/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 out.2024.

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

FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). **Tecnologia jurídica & direito digital**: II congresso internacional de direito, governo e tecnologia – 2018. Belo Horizonte: Fórum, 2018.

GARCIA, Marco. **Big Data: O que é, conceito e definição.** Publicado em: 26 de janeiro de 2022. Disponível em: https://cetax.com.br/big-data/. Acesso em: 12 out.2024.

GARFINKEL, Simson. **Database Nation**: The Death of Privacy in the 21th Century. O'Reilly Media: California, 2000.

MANDARINO JUNIOR, R. **Segurança e defesa do espaço cibernético brasileiro.** Recife: Cubzac, 2010.

MAGRO, Américo Ribeiro. **A (in)eficácia do direito à anonimização de dados pessoais em face da análise de big data dos metadados produzidos no âmbito da internet das coisas.** In: TEIXEIRA, Tarcísio; MAGRO, Américo Ribeiro (coord.). Proteção de dados fundamentos jurídicos. Salvador, Juspodivm, 2020, p. 53-86.

MARCONDES, Juliana. **Quem é o Data ProtectionOfficer?**. Publicado em: 2017. Disponível em: http://www.plmj.com/xms/files/2017_PDF/junho/Quem_e_o_Data_Protection_Officer.pdf. Acesso em: 18 out.2024.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. **Autodeterminação informativa e responsabilização proativa**: novos instrumentos de tutela da pessoa humana na LGDP. Rio de Janeiro: Anja Czymmeck, 2019.

MARTINS, Leonardo. (org.) **Cinquenta anos de Jurisprudência do Tribunal Constitucional Federal Alemão.** Montevidéu: Fundação Konrad Adenauer, 2005.

NAKATA, Alexandre. A responsabilidade civil de provedores de aplicação de internet à luz da Lei de Proteção de Dados Pessoais e do Código de Defesa do Consumidor. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 24, n. 5989, 24 nov. 2019. Disponível em: https://jus.com.br/artigos/69968. Acesso em: 23 out.2024.

OLIVEIRA, Ana Paula de; ZANETTI, Dânton, LIMA, Flávio Santos. A lei geral de proteção de dados brasileira na prática empresarial. **Revista Jurídica da Escola Superior de Advocacia da OAB-PR.** Ano 4, n. 1, p. 1-29, maio de 2019.

PEZZI, Ana Paula Jacobus. **A necessidade de Proteção de Dados Pessoais nos arquivos de Consumo**: em busca da concretização do direito à privacidade. São Leopoldo, 2017.

PINHEIRO, Patrícia Peck. **Direito Digital.** São Paulo: Editora Saraiva, 2021.

SANTOS, Manoel J. Pereira dos. Responsabilidade civil pelos ilícitos informáticos típicos. In: SILVA, Regina Beatriz Tavares da; SANTOS, Manoel J. Pereira dos, (coord.) **Responsabilidade civil**: responsabilidade civil na internet e nos demais meios de comunicação. 2. ed. São Paulo: Saraiva, 2012.

SARMENTO, Daniel; GALDINO, Flávio. **Direitos Fundamentais**: estudos em homenagem ao professor Ricardo Lobo Torres. Rio de Janeiro: Renovar, 2014.

SCHWAB, Klaus. **A quarta revolução industrial.** Tradução por Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SOFTWALL SOLUÇÕES EM TECNOLOGIA. **Vazamento de dados e suas consequências para empresas.** Publicado em: 12 de março de 2019. Disponível em: https://www.softwall.com.br/vazamento-dedados-e-suas-consequencias-para-empresas/. Acesso em: 22 out.2024.

LIMBERGER, Têmis. Cibertransparência - Informação Pública em Rede - A virtualidade e suas repercussões na realidade. 01. ed. Porto Alegre: Livraria do Advogado, 2016.

TOMASEVICIUS FILHO, Eduardo. **A Lei Geral de Proteção de Dados Brasileira.** Coimbra, Portugal: Grupo Almedina (Portugal), 2021.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sergio Antonio Fabris Editora, 2017.

VERÍSSIMO, Carla. **Compliance**: incentivo à adoção de medidas anticorrupção. São Paulo: Saraiva, 2017.