CENTRO UNIVERSITÁRIO SOCIESC DE BLUMENAU – UNISOCIESC

CAROLINE ALVES DE SOUZA

LEI GERAL DE PROTEÇÃO DE DADOS E SEUS DESAFIOS NO ÂMBITO EMPRESARIAL

Blumenau
2023

CAROLINE ALVES DE SOUZA

LEI GERAL DE PROTEÇÃO DE DADOS E SEUS DESAFIOS NO ÂMBITO EMPRESARIAL

Trabalho de Conclusão de Curso apresentado ao curso de graduação em Direito, do Centro Universitário Sociesc de Blumenau - UNISOCIESC, como requisito parcial para obtenção de título de bacharel. Orientadora: Prof.ª Silvia Helena Arizio

Blumenau
2023

AGRADECIMENTOS

Gostaria de aproveitar este espaço para expressar minha profunda gratidão a todas as pessoas que contribuíram na minha jornada desta graduação tornando possível escrever e realizar este Trabalho de Conclusão de Curso. Este projeto representou um desafio significativo em minha jornada acadêmica, e não teria sido bem-sucedido sem o apoio e contribuições de todos os envolvidos.

Primeiramente, quero agradecer à minha família, que sempre esteve ao meu lado com amor, paciência e incentivo inabalável. Vocês foram minha fonte de força e inspiração durante todo esse processo.

A minha orientadora, Silvia Helena Arizio, deixo minha profunda gratidão por sua orientação para estruturar esse projeto. Suas sugestões e insights me levaram a uma maior compreensão e pesquisa.

Aos meus amigos e colegas, que compartilharam experiências e apoio emocional, deixo um grande obrigado, por toda troca em conversas.

Aos meus companheiros de vida, do dia a dia e dessa jornada, que foram um dos grandes incentivadores a desenvolver esse projeto, Jonathan e Don, em que estiveram ao meu lado nos momentos de dúvidas, incertezas e nos momentos em que foram horas escrevendo esse projeto.

A todos vocês, minha gratidão é profunda e genuína. Este trabalho não seria possível sem o apoio e envolvimento de cada um de vocês. Obrigado por fazerem parte desta jornada.

RESUMO

Tendo em vista que a implementação da Lei Geral de Proteção de Dados (LGPD) no âmbito empresarial pode trazer alguns desafios e preocupações isso, pode exigir investimentos significativos em tecnologia, infraestrutura, treinamento de funcionários e consultoria jurídica, em que representa muitas das vezes um custo financeiro para as empresas, especialmente as de menor porte, que podem encontrar dificuldade em absorver as despesas adicionais, optou-se por analisar os desafios enfrentados pelas empresas na adequação aos requisitos da LGPD frente a elaboração e execução dos contratos nos quais também incluem a revisão de contratos existentes, incluindo redação clara e precisa, com a garantia da conformidade de terceiros contratados e a prevenção de penalidades. Para tanto, foi necessário a aplicação do método indutivo e a metodologia através de pesquisas bibliográficas, documentais e legislativas. O trabalho constata (1) quais são os desafios enfrentados pelas empresas na adequação aos requisitos da LGPD (2); a necessidade de revisar os contratos existentes para garantir que estejam em conformidade com a LGPD; (3) inclusão de cláusulas específicas relacionadas ao tratamento de dados pessoais. Também, irá verificar (4) como as empresas podem garantir que os contratos em questão sejam redigidos de forma clara e precisa, para que não haja ambiguidade quanto às obrigações e responsabilidades das partes envolvidas no tratamento dos dados pessoais. (5) Além de destacar como a LGPD estabelece penalidades significativas para empresas que não cumprem seus requisitos. Portanto, a elaboração e execução de contratos em conformidade com a LGPD é crucial para evitar multas e danos à reputação da empresa.

Palavras-chave: Adequação Normativa; LGPD; Obrigação e Responsabilidades no Tratamento de Dados Pessoais;

ABSTRACT

Bearing in mind that the implementation of the General Data Protection Law (LGPD) at the business level can bring some challenges and concerns, it may require investments in technology, infrastructure, employee training and legal consultancy, which often represents a financial cost For companies, especially smaller ones, which may find it difficult to absorb additional expenses, it was decided to analyze the challenges faced by companies in adapting to LGPD requirements in the preparation and execution of contracts which also include the review of existing contracts, including clear and precise wording, with guarantee of compliance of contracted third parties and prevention of losses. To this end, it was necessary to apply the inductive method and methodology through bibliographical, documentary and legislative research. The work will establish (1) what are the challenges faced by companies in complying with LGPD requirements (2); the need to review existing contracts to ensure they comply with the LGPD; (3) inclusion of specific clauses related to the processing of personal data. Also, I will look at (4) how companies can ensure that the contracts in question are written clearly and precisely, so that there is no ambiguity regarding the obligations and responsibilities of the parties involved in the processing of personal data. (5) In addition to highlighting how the LGPD establishes significant provisions for companies that do not meet its requirements. Therefore, drafting and executing contracts in compliance with the LGPD is crucial to avoid fines and damage to the company's concession.

Keywords: LGPD; Obligation and Responsibilities in the processing of personal data; Regulatory adequacy;

SUMÁRIO

INTRODUÇÃO.....7

2 BREVE ANÁLISE DO DIREITO DIGITAL NA SOCIEDADE IA.....9

2.1 INTRODUÇÃO AO DIREITO DIGITAL.....10

2.2 CONCEITOS FUNDAMENTAIS: INTELIGÊNCIA ARTIFICIAL.....11

2.3 IMPACTOS DA INTERNET.....13

3. DIREITO DIGITAL E MARCO REGULATÓRIO.....15

3.1 DOS DIREITOS E GARANTIAS DOS USUÁRIOS.....16

3.2 CATEGORIAS DE ARMAZENAMENTO DE DADOS.....17

3.3 LEGISLAÇÕES PERTINENTES.....18

4 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).....21

4.1 PROTEÇÃO DE DADOS PESSOAIS: FUNDAMENTOS TEÓRICOS E HISTÓRICOS.....22

4.2 CONCEITOS, PRINCÍPIOS E INSTITUTOS DA LGPD. DO TRATAMENTO DE DADOS PESSOAIS E DOS DIREITOS DO TITULAR. DA SEGURANÇA E DAS BOAS PRÁTICAS.....23

4.3 APLICAÇÃO DA LGPD NAS EMPRESAS.....26

5 DESAFIOS PARA APLICAÇÃO DA LGPD NAS ORGANIZAÇÕES EMPRESARIAIS.....27

5.1 ADAPTAÇÃO DAS EMPRESAS E ORGANIZAÇÕES À LGPD.....28

5.1.1 Desafios técnicos e operacionais para a implementação da LGPD.....30

5.2 CONTRATOS EMPRESARIAIS: ADEQUAÇÕES.....32

5.2.1 Função social do contrato.....33

5.2.2 Princípios basilares e elementos essenciais de uma relação contratual.....35

5.2.3 Responsabilidade civil na LGPD: subjetiva ou objetiva?.....36

5.3 EXTINÇÃO DO CONTRATO.....38

5.3.1 Consequências jurídicas em caso de descumprimento da LGPD.....38

5.3.2 Multas contratuais vs. Multas administrativas da ANPD.....39

CONSIDERAÇÕES FINAIS.....41

REFERÊNCIAS.....42

INTRODUÇÃO

O Direito Digital é uma área do direito que se concentra na regulamentação das atividades relacionadas à internet, tecnologia da informação e dados digitais. Ele abrange uma variedade de questões legais que surgem com o avanço da tecnologia e o uso cada vez mais difundido da internet, como a privacidade, segurança cibernética, comércio eletrônico, propriedade intelectual online e muitos outros.

Nas últimas décadas, houve um rápido avanço na tecnologia da informação, com a disseminação da internet, dispositivos móveis, redes sociais, computação em nuvem e big data, com isso, houve a criação de novas oportunidades e desafios legais que precisaram ser abordados.

A internet tornou-se uma transcendente de fronteiras geográficas, produzindo efeitos de questões legais no âmbito digital muitas vezes internacionais. O Direito Digital atende questões de jurisdição, tratados internacionais e cooperação entre países, sendo um tema importante que norteia o mundo inteiro, com isso, a coleta, armazenamento e uso de dados pessoais estão no centro das preocupações do Direito Digital. Regulamentos como o GDPR na União Europeia e leis de privacidade de dados em outros lugares estão moldando a forma como as empresas e organizações podem lidar com informações pessoais.

O Direito Digital não é apenas sobre regulamentação, mas também sobre educar os cidadãos e empresas sobre seus direitos e responsabilidades. Sendo assim, a importância do Direito Digital na era da tecnologia da informação reside na necessidade de estabelecer regras claras e justas para lidar com questões complexas e em constante evolução no ambiente digital. Isso garante a proteção dos direitos individuais, segurança online e governança eficaz da tecnologia da informação, promovendo um ambiente digital seguro e responsável para todos os envolvidos.

Dentre eles, uma legislação “nova” em que foi aprovada e classificada com o seu nome em agosto de 2018, entrando em vigor somente em 2020, foi a lei n°13.709/2018, referente a LEI Geral de Proteção de Dados (LGPD), no âmbito do Direito Digital, a LGPD, no qual visa estabelecer regras e diretrizes para o tratamento de dados pessoais por parte de empresas e organizações, com intuito de proteger a privacidade e os direitos individuais. Neste contexto, serão abordados os principais desafios e perspectivas para a aplicação da

LGPD no ambiente digital, considerando a necessidade de adaptação das empresas, a proteção dos direitos dos usuários e as possíveis consequências jurídicas em caso de descumprimento da lei.

O direito à privacidade é um direito fundamental que garante a proteção da vida privada e intimidade das pessoas. No âmbito contratual, esse direito ganha ainda mais importância, uma vez que as informações pessoais dos contratantes podem ser compartilhadas e utilizadas pelas partes envolvidas no contrato.

O objetivo geral será analisar os desafios enfrentados pelas empresas na adequação aos requisitos da LGPD na elaboração e execução de contratos em que incluem a revisão de contratos existentes, a redação clara e precisa dos contratos, a garantia da conformidade de terceiros contratados e a prevenção de penalidades.

Nesse contexto, surge o seguinte questionamento: A conscientização governamental das empresas dialoga na implementação da Lei 13.709/2018? Como fica a estruturação no quesito empresarial?

Tem-se como hipóteses: a educação referente a temática para as organizações privadas que enfrentam uma certa dificuldade em implementar processos e regularizar seus fluxos de acordo que se faz necessário uma especialização nesta área para alcançar êxito neste desafio. Sendo assim, faz-se necessário despender muitas das vezes, tempo, investimentos financeiros e pessoas especializadas e capacitadas para regularização nos termos da Lei 13.709/2018.

Como segunda hipótese, a LGPD introduz uma série de requisitos e obrigações que podem ser complexos de entender e implementar. As empresas podem ter dificuldades em mapear seus processos de coleta, uso e armazenamento de dados pessoais, além de precisarem adotar medidas de segurança e proteção adequadas. A falta de compreensão e capacitação adequada pode levar a erros na implementação, resultando em não conformidade e possíveis sanções.

Para o desenvolvimento deste trabalho, o método de pesquisa utilizado é o indutivo pois serão apresentados quais são os desafios enfrentados pelas empresas na adequação frente a essa normativa objetivando a efetividade assertiva desse tema. Assim sendo, a pesquisa tem caráter bibliográfico e documental, com a análise de livros, normativas legislativas, exploratórias e divulgados em meios eletrônicos e outros meios que se apresentam importantes.

Os três primeiros capítulos trarão a abordagem sobre o direito digital na sociedade, com os fundamentos do Marco Civil da Internet e os principais eventos que resultaram historicamente nesse marco com suas especificidades e desdobramentos, também abordará os Fundamentos do Direito Digital com ênfase em suas características e normativas nacionais e internacionais e sobre a Lei Geral de Proteção de Dados apresentando o conceito e, fazendo uma análise posteriormente aplicada de seus princípios e diretrizes no âmbito empresarial enfatizando as responsabilidades ao tratamento de dados e seus titulares, bem a historicidade da Lei Geral de Proteção de dados, com seus conceitos, fundamentos, princípios, instituições e estruturação de tratamento dos dados.

Nos capítulos posteriores, o estudo será direcionado para os desafios da aplicação da LGPD no ambiente digital frente a implementação nas empresas, bem como, as consequências jurídicas em caso de descumprimento da lei. Ainda, as perspectivas para o Direito Digital e a LGPD diante dos avanços tecnológicos e suas aplicações através da importância acerca da conscientização e educação digital.

Por fim, trará como desfecho uma breve análise sobre todo o trabalho construído com suas considerações finais.

2 BREVE ANÁLISE DO DIREITO DIGITAL NA SOCIEDADE IA

A indústria 4.0, também conhecida como a quarta revolução industrial, vem estabelecendo nas empresas a implementação de inovações tecnológicas tanto para as automatizações da cadeia de produção, como no ambiente de trabalho. Tais inovações têm como objetivo tornar a produção mais eficiente e otimizada.

As inovações inseridas na indústria 4.0 que serão discorridas no decorrer deste trabalho, representam métodos para análises de dados, personalização em larga escala entre outros, para ampliação da digitalização ao alcance de boa parte da humanidade atrelando-se intrinsecamente a sociedade 5.0, nas quais desempenham um papel para a transformação no modo de vida das pessoas, com objetivo de buscar resolver problemas sociais, econômicas e ambientais. (STEFANINI, 2022). Tais mudanças tomaram forças devido ao ambiente de troca de informações de forma rápida e fácil, possibilitando o atingimento dos objetivos em prol do ser humano.

A Quarta Revolução Industrial, segundo SCHWAB (2019), é totalmente diferente das revoluções industriais anteriores, com transformações de velocidade, amplitude, profundidade e impacto sistêmico. As revoluções industriais anteriores seguiam determinadas bases de fontes principais de energia para produção em série, como foi o caso das máquinas a vapor e da eletricidade.

A internet das coisas (IoT) é um componente central da Revolução 4.0, envolvendo a conexão de objetos e dispositivos à internet, permitindo a coleta e a troca de dados em tempo real. Com isso, possibilita uma visão ampla para tomada de decisões de diversos setores.

Contudo, a inteligência artificial (IA) desempenha um papel fundamental nesta Revolução, trazendo um aprendizado de máquina tornando-os mais inteligentes e capazes de tomadas de decisões com base em dados. Tal resultado possui aplicação em diversas áreas, como automação de processos, análise de dados e muito mais.

Outrossim, com tal avanço criou-se uma transformação de mercado, onde a IA têm o potencial de automatizar empregos, em contrapartida, oportunizando novas vagas com manutenção, programação e supervisão desses sistemas automatizados.

Portanto, a Revolução 4.0 é um fenômeno em constante evolução, e suas implicações ainda estão sendo compreendidas e implementadas em todo o mundo. Possui um potencial de trazer benefícios significativos, mas também levanta desafios e questões éticas que devem ser abordados para garantir um futuro sustentável e eficiente, tendo impacto em vários setores, trazendo mudanças de como estes irão se adaptar às demandas do século XXI.

2.1 INTRODUÇÃO AO DIREITO DIGITAL

O Direito Digital vem sendo considerado uma nova disciplina jurídica. Sua idade é estimada em duas décadas. Costuma-se dizer que a Portaria Interministerial 147, de 31 de maio de 1995, editada pelos ministros da Comunicação e da Ciência e Tecnologia, que regulou o uso de meios da rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet, foi o primeiro diploma legal desse ramo (ARAÚJO, 2017, p. 17).

A pesquisa do Prof. João Marcello de Araújo Jr., apresentado no Congresso de Würzburg (Alemanha), em outubro de 1992, demonstrou, entretanto, que, pelo menos desde 1976, a Câmara dos Deputados e o Senado tramitam projetos de lei que tratavam de informática. São exemplos: o projeto de lei no 3.279, de 1976, do Deputado Siqueira Campos, que dispunha "sobre a programação viciada de computador"(arquivado em 1979); o projeto de lei no 96, de 1977, do Senador Nélson Carneiro, que dispunha "sobre a proteção das informações computadorizadas" (arquivado em 1980); projeto de lei no 579, de 1991, do Deputado Sólon Borges dos Reis, que dispunha "sobre o crime de interferência nos sistemas de informática (destruição); entre outros (REIS, 1997, p. 50).

O Direito Digital nasceu da necessidade de se regularem as questões surgidas com a evolução da tecnologia e a expansão da internet, elementos responsáveis por profundas mudanças comportamentais e sociais, bem como para fazer frente aos novos dilemas da denominada "Sociedade da Informação", este termo foi propagado em sua maior parte, pelo sociólogo Manuel Castells. (MAIS, Equipe, 2021)

A doutrina tem assinalado um aspecto interessante desse ramo do Direito que afirma que o Direito Digital não tem objeto próprio. Seria um Direito com um "modus operandi diferente, sendo, na verdade, a extensão de diversos ramos da ciência jurídica, que cria novos instrumentos para atender aos anseios e ao aperfeiçoamento dos institutos jurídicos em vigor" (ARAÚJO, 2017, p. 24).

De acordo com Patrícia Peck Pinheiro, o Direito Digital é a evolução do próprio Direito e abrange "todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas" (2008, p. 29).

2.2 CONCEITOS FUNDAMENTAIS: INTELIGÊNCIA ARTIFICIAL

Ao falar sobre tecnologia da informação existem termos essenciais para entender como funcionam os sistemas e as máquinas. Para o Direito, essa conceituação é indispensável, pois os regramentos e as decisões judiciais levam em consideração o significado de cada termo e a que se refere.

Segundo SILVA, (2021) os “algoritmos” são imprescindíveis para os sistemas digitais. Caracterizam-se por conter, obrigatoriamente, uma norma estabelecida para um procedimento que, quando empregado, produzirá um resultado, passando por algumas etapas. Assim, os algoritmos formam uma sequência de atos lógicos, raciocínios, instruções, operações, todos ordenados para alcançar um objetivo, de modo que todas as etapas devem ser seguidas. Além disso, os algoritmos desempenham um papel decisor sendo utilizados para respostas de questões objetivas e, ainda, para decidir sobre questões subjetivas, complexas e que envolvem juízos sofisticados de valor, como estas: Quem deve ser contratado para trabalhar em uma empresa? Que contrato deve ser celebrado e em quais bases? Qual é a probabilidade de reincidência de determinado criminoso?

Por outro lado, os dados são as informações coletadas, inseridas e fornecidas para determinada finalidade. Atualmente, essas informações abastecem os algoritmos, tendo como principal ativo boa parte das organizações, movimentando a economia digital. Portanto, proteger os dados é uma forma de proteger os cidadãos e a sociedade de modo a estabelecer que tais previsões legais demonstram como os dados devem ser tratados, quais são os direitos e obrigações das pessoas físicas e jurídicas, consequências dos descumprimentos, entre outros. (SILVA, Louise S.H Thomaz Da, 2021, pg. 26)

Paralelamente, a inteligência artificial é utilizada com o intuito de automatizar determinados processos executados por humanos, através de automatização de máquinas a aprender um processo, chamado “machine learning”, visando simular o pensamento humano para tomada de decisões, execução de tarefas, entre várias outras aplicabilidades de forma autônoma. A inteligência, é abastecida com os dados, através de algoritmos, produzindo previsões, entretanto, as decisões automatizadas também têm potencial para violar os direitos fundamentais, o que pode ser minimizado pelo cumprimento de determinados parâmetros éticos e legais que assegurem a transparência a respeito do uso das informações, bem como a correção e atualização das informações que servem como input do algoritmo.

SILVA, Louise S.H Thomaz Da (2021, pg. 27) Acrescenta um termo muito utilizado quando o assunto é tecnologia chamado de “Big data”. Esse termo refere-se a uma grande quantidade de dados de forma diversificada, com fontes variadas tendo um processamento rápido comparada a grande quantidade de dados. Incluso a esses “grandes” dados, os dados pessoais também integram a big data, sendo a LGPD extensiva a ele.

Do mesmo modo, com a evolução da tecnologia questões financeiras foram mudando a forma que se movimenta a economia mundial. O que era no passado a moeda de utilizar o dinheiro em papel, passou a ser cada vez mais tecnológico na sociedade. Dito isso, o blockchain foi desenvolvido para apoiar as áreas financeiras e empresariais, promovendo garantias, como a segurança jurídica para os smart contracts, funcionando através de blocos de informações regidos por um código, auto executável, que permite a negociação e a execução de um contrato. (SILVA, Louise S.H Thomaz Da, 2021, pg. 28)

Nesse sentido, é importante falar sobre a cidadania digital, no qual se refere aos exercícios de direitos por parte dos indivíduos. Sob a ótica do Direito Digital, à medida que um cidadão digital consome dados, fornece dados e tem acesso a todo momento por meio de informações é necessária a observância aos princípios da privacidade, intimidade e liberdade de expressão. Todavia, tais princípios não devem servir de justificativa para constranger o outro. A ética e a boa-fé objetiva devem prevalecer tanto nas relações pessoais quanto nas relações virtuais. (SILVA, Louise S.H Thomaz Da, 2021, pg. 29).

2.3 IMPACTOS DA INTERNET

Considerando que o avanço da Internet está presente na vida de milhares de pessoas, seus impactos repercutem em todas as esferas jurídicas. Dessa forma, cabe ao profissional que trabalha com Direito Digital, estar atento aos pontos sensíveis das diversas matérias que abarcam o direito.

Um dos cenários que trazem impactos através da internet é a privacidade. Fato é que a vida em sociedade está cada vez mais inserida em um mundo altamente conectado, que ultrapassa barreiras físicas e onde se utiliza diversas vezes aplicações gratuitas, sem saber, exatamente, para onde tais dados estão indo ou sendo armazenados e tratados.

Dessa forma, é dificultosa a tarefa de garantir plena proteção aos dados e privacidade, sendo que as fundamentações para proposição de ações encontram-se na interpretação extensiva de códigos diferenciados como: Direito do Consumidor, Direito Civil, Marco Civil da Internet e princípios constitucionais. No entanto, tende a se amenizar com a entrada em vigor da LGPD (Lei Geral de Proteção de Dados).

A liberdade de expressão é um direito fundamental que deve ser protegido tanto na vida real quanto na internet. No entanto, a segurança da informação na internet é uma preocupação crescente, pois, muitas vezes, as informações compartilhadas podem ser usadas para fins maliciosos. É importante encontrar um equilíbrio entre a proteção da liberdade de expressão e a segurança da informação. (TRUZZI, Gisele. PALOTTA, Iasmin, 2023).

De acordo com RUZZI, Gisele. PALOTTA, Iasmin, (2023), o Direito Digital enfrenta diversos desafios em sua aplicação e evolução. Alguns deles incluem:

1. Regular o uso da tecnologia: A rapidez da evolução tecnológica torna difícil para o Direito acompanhar e regular o uso da tecnologia de maneira eficaz.
2. Proteção de dados pessoais: O aumento da coleta e armazenamento de dados pessoais exige que sejam estabelecidas normas claras sobre a proteção desses dados e o uso que pode ser feito deles.
3. Conflitos de jurisdição: Na era digital, os conflitos podem surgir em diferentes jurisdições, tornando difícil determinar o local adequado para solução de disputas.
4. Questões de privacidade: A privacidade na era digital é um assunto complexo, com muitas questões ainda sem resposta sobre o que é aceitável e o que não é.
5. Neutralidade da rede: A neutralidade da rede é uma questão importante, pois trata da igualdade de acesso à Internet e à informação.
6. Propriedade intelectual: O Direito Digital precisa equilibrar os direitos de propriedade intelectual com a liberdade de expressão e o acesso à informação.

Sendo assim, a internet trouxe uma série de benefícios que impactaram positivamente a sociedade, entre eles a democratização do conhecimento. Impulsionou os comércios eletrônicos, também permitindo educação à distância no formato online. Entretanto, esses são apenas alguns dos desafios enfrentados pelo Direito Digital, e é importante continuar a debater e buscar soluções para garantir que as leis se mantenham relevantes e aplicáveis na era digital. (TRUZZI, Gisele. PALOTTA, Iasmin, 2023).

3. DIREITO DIGITAL E MARCO REGULATÓRIO

O Direito Digital é uma área do Direito que trata de questões relacionadas ao uso da tecnologia da informação e da internet, incluindo tópicos como privacidade, proteção de dados, propriedade intelectual, direitos autorais, entre outros. É importante destacar que o Direito Digital é uma área interdisciplinar, envolvendo tanto questões de Direito quanto questões técnicas. (TRUZZI, Gisele. PALOTTA, Iasmin, 2023).

Com todo o avanço tecnológico observou-se a necessidade de regulamentar o uso da internet para sociedade, com seus direitos e deveres.

No Brasil, o Marco Civil da Internet, teve como oficialmente uma das primeiras leis criadas com o objetivo de proteger o usuário da lei conhecida como Lei nº 12.965/2014, que se trata de uma legislação brasileira que estabelece princípios, direitos e deveres para o uso da internet no Brasil. Ele foi aprovado e sancionado em abril de 2014 e é frequentemente considerado um dos mais avançados marcos legais relacionados à internet em todo o mundo. O Marco Civil tem como objetivo principal garantir a liberdade, a privacidade e a neutralidade da rede no ambiente online brasileiro. Conforme o inciso I do Artigo 5° da Lei n° 12.965/2014, internet é: "[...] o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".

Outro marco importante do Direito Digital no Brasil é a chamada "Lei Carolina Dieckmann". Esta lei foi criada em 2012 e tem como objetivo proteger as vítimas de crimes cibernéticos, tais como invasão de privacidade e vazamento de informações pessoais. Esta lei criou crimes específicos e estabelece penas para esses delitos, permitindo às vítimas buscarem reparação por meio do Judiciário. (TRUZZI, Gisele. PALOTTA, Iasmin, 2023).

A Lei Geral de Proteção de Dados (LGPD) é outro importante marco regulatório do Direito Digital no Brasil. Aprovada em 2018, a LGPD tem como objetivo proteger os dados pessoais dos cidadãos e estabelecer regras para coleta, tratamento e armazenamento de dados pessoais. A lei também estabelece sanções para empresas que descumprirem as regras de proteção de dados. (TRUZZI, Gisele. PALOTTA, Iasmin, 2023).

Portanto, com esses avanços o Brasil passou por marcos regulatórios no âmbito do direito digital, visando a maior regulamentação dos direitos e deveres da sociedade.

3.1 DOS DIREITOS E GARANTIAS DOS USUÁRIOS

O Marco Civil da Internet, no Brasil, estabelece direitos e garantias dos usuários da internet com o objetivo de assegurar um ambiente digital que promova a liberdade, a privacidade, a neutralidade da rede e a participação ativa dos cidadãos.

Dentre os direitos e garantias dos usuários, pode-se citar alguns elementos como:

(1) Neutralidade da Rede, no Brasil, a neutralidade de rede é assegurada na lei que ficou conhecida como Marco Civil da Internet (nº 12.965, de 2014). O Artigo 3º lista a neutralidade como um dos princípios da lei. O Artigo 9º estabelece que "o responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação". (AGÊNCIA BRASIL, 2023)

(2) Privacidade e Proteção de Dados: A lei garante a privacidade dos usuários, estabelecendo que a coleta, o armazenamento e o tratamento de dados pessoais devem ser realizados com consentimento do usuário ou por determinação legal. Os usuários têm o direito de acessar, corrigir e excluir seus dados pessoais. Em poucas palavras, a proteção de dados é sobre a proteção de dados contra acesso não autorizado. Privacidade de dados é sobre acesso autorizado — quem tem e quem define. (PROGRESS FORMELY IPSWITCH, 2023)

(3) Liberdade de Expressão: A lei geral de proteção de dados não traz novidades ou inovações no tocante propriamente à liberdade de expressão, e sim, vem ratificar a sua importância perante o mundo jurídico e social. (TEIXEIRA, Ilderlandio, 2020)

(4) Responsabilidade por Conteúdo: A responsabilidade civil do provedor de internet pelos danos decorrentes do conteúdo gerado por terceiro é subsidiária e ocorrerá em caso de descumprimento de ordem judicial que determinar a indisponibilização do conteúdo ilícito ou da permanência de imagens/vídeos íntimos após a ciência do ocorrido. Tais sujeitos não realizam controle prévio de material disponibilizado na rede. (TJDFT, 20221).

(5) Acesso Universal é o direito de todos os cidadãos ao acesso à internet como um serviço essencial. O Estado é responsável por promover o acesso à rede em áreas sem cobertura, conforme Lei n°12.527/11.

(6) Participação Social, a Lei nº 13.709/2018 prevê a participação da sociedade civil e da comunidade tecnológica no processo de definição de políticas relacionadas à internet no Brasil. Isso inclui a realização de consultas públicas e debates sobre questões relevantes.

(7) Proteção contra Abusos, os usuários têm o direito de denunciar abusos e práticas ilegais na internet, como difamação, discurso de ódio, cyberbullying e violações de privacidade. As autoridades devem investigar esses casos e tomar medidas legais apropriadas, conforme disposto no Art. 5°, XI da Lei nº 13.709/2018.

(8) Transparência, os provedores de serviços online devem fornecer informações claras e transparentes sobre suas políticas de privacidade, termos de uso e práticas de coleta de dados conforme disposto no Art. 10°,§2° da Lei nº 13.709/2018, .

(9) Responsabilidade por Danos, os provedores de serviços online podem ser responsabilizados por danos causados aos usuários devido a falhas na prestação de serviços ou violações da legislação, incluindo violações de privacidade, conforme Seção III, da Lei nº 13.709/2018.

(10) Portabilidade de Dados, os usuários têm o direito de solicitar a portabilidade de seus dados pessoais entre diferentes serviços online, facilitando a mudança de plataformas sem perder suas informações no Art. 11°, §4°, I da Lei nº 13.709/2018.

É de suma importância que os usuários estejam cientes de seus direitos e exerçam essas garantias quando necessário. Além disso, as empresas que operam na internet devem estar em conformidade com as disposições do Marco Civil da Internet para proteger os direitos e interesses dos usuários. Em casos de violações, os usuários possuem recursos legais disponíveis para buscar reparação e justiça.

3.2 CATEGORIAS DE ARMAZENAMENTO DE DADOS

O armazenamento de dados é uma das partes fundamentais da tecnologia, onde os dados podem ser armazenados de diversas maneiras, com base em vários critérios, como finalidade, capacidade e custo. Cada tipo de armazenamento tem suas vantagens e desvantagens, dependendo dos requisitos específicos de um sistema, como capacidade, velocidade, durabilidade entre outros.

Segundo o site IBM (2023) para armazenar dados, independentemente da forma, os usuários precisam de dispositivos de armazenamento. Os dispositivos de armazenamento de dados dividem-se em duas categorias principais: armazenamento de área direto e armazenamento em rede.

Cada categoria de armazenamento de dados está interligada intrinsecamente com o direito, especialmente no que diz respeito à privacidade, segurança, regulamentação e propriedade de dados. As leis de privacidade de dados variam de país para país, considerando a transferência internacional de dados entre jurisdições diferentes nas quais estão sujeitas a restrições e acordos específicos. Portanto, as categorias de armazenamento de dados estão relacionadas com as leis regulamentadoras que afetam a coleta, armazenamento e processamento dos dados, para que assegure a garantia dos direitos individuais, bem como, que as obrigações legais sejam respeitadas.

3.3 LEGISLAÇÕES PERTINENTES

Segundo a Secretária da Ciência, Tecnologia e Inovação (2022), as legislações pertinentes referem-se às leis, regulamentos e normas que são relevantes e aplicáveis na esfera do Direito Digital e a sua área de atuação. Com isso, define as regras, obrigações e direitos que legislam a este determinado assunto e situação deste segmento que envolve a sociedade num todo. Entretanto, os conceitos de legislações podem variar de acordo com o contexto em que se enquadram.

Na esfera em que compete ao poder legislativo, como o Congresso Nacional ou o Parlamento, as leis nas quais são promulgadas podem ser em três níveis, sendo estes: federal, estadual ou municipal.

No que tange ao Direito Digital, temos as Leis Distritais, com as seguintes previsões:

> Lei nº 6.519/2020 – Dispõe sobre normas específicas de proteção e defesa dos direitos dos usuários dos serviços públicos distritais e de participação dos usuários na fiscalização da eficácia desses serviços e regulamenta o art. 30 da Lei Orgânica do Distrito Federal. Recepciona a Lei n. 13.460/2017 no âmbito do Distrito Federal. (BRASÍLIA 2020);
> Lei nº 4.896/2012 – Lei do SIGO/DF – Dispõe sobre o Sistema de Gestão de Ouvidoria do Distrito Federal – SIGO/DF. (BRASÍLIA 2012);
> Lei nº 4.990/2012 – Lei de Acesso à Informações no DF – Regula o acesso a informações no Distrito Federal previsto no art. 5º, XXXIII, no art. 37, § 3º, II, e no

> art. 216, § 2º, da Constituição Federal e nos termos do art. 45, da Lei federal nº 12.527, de 18 de novembro de 2011, e dá outras providências. (BRASÍLIA 2012);

Na esfera federal, temos as legislações previstas:

> Lei n° 13.460/2017 – Lei dos Usuários dos Serviços Públicos – Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. (BRASIL, 2017)
> Lei nº 12.527/2011 – Lei de Acesso à Informação Pública – Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. (BRASIL, 2011)

Sob a ótica de regulamentos que envolvem regras e diretrizes elaboradas por agências governamentais ou autoridades reguladoras para implementar e detalhar as disposições das leis, ou muitas das vezes, dispõe de regulamentos que elucidam da melhor forma como as leis devem ser aplicadas na prática, temos os decretos com tais previsões:

> Decreto n° 39.723/2019 – Estabelece medidas, no âmbito no Sistema de Gestão de Ouvidoria do Distrito Federal, para garantir a efetividade da participação popular no aprimoramento dos serviços públicos prestados pela Administração Pública direta e indireta do Distrito Federal, e dá outras providências. (DISTRITO FEDERAL/DF, 2019);
> Decreto n° 36.462/2015 – Regulamenta a Lei nº 4.896, de 31 de julho de 2012, que dispõe sobre o Sistema de Gestão de Ouvidoria do Distrito Federal – SIGO/DF. (DISTRITO FEDERAL/DF, 2015);
> Decreto nº 36.419/2015 - Institui a Carta de Serviços ao Cidadão. (DISTRITO FEDERAL/DF 2015);
> Decreto nº 35.382/2014 – Regulamenta o art. 42, da Lei nº 4.990, de 12 de dezembro de 2012, dispõe sobre os procedimentos para credenciamento de segurança, sobre o Núcleo de Segurança e Credenciamento, institui o Comitê Gestor de Credenciamento de Segurança, e dá outras providências. (DISTRITO FEDERAL/DF 2014);
> Decreto nº 34.276/2013 – Regulamenta a Lei nº 4.990, de 12 de dezembro de 2012, que dispõe sobre o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do §3º do art. 37 e no §2º do art. 216, todos da Constituição Federal de 1988. (DISTRITO FEDERAL/DF 2013);

Outrossim, as Instruções Normativas são padrões estabelecidos por organizações públicas para garantir a qualidade e segurança de produtos ou serviços em uma determinada esfera, seja indústria ou campo. Tais normas podem ser obrigatórias ou voluntárias, com isso, na esfera no Direito Digital às Instruções Normativas visam regulamentar os procedimentos digitais, bem como, institui termos e metodologias a serem seguidas e suas disciplinas para realização de seus processos. Dentre eles, nessa esfera temos as normativas abaixo:

> Instrução Normativa n° 01/2018 – Regulamenta os procedimentos de restrição de acesso à informação que possuam algum impedimento legal, nos termos da Lei nº 4.990/2012 regulamentada pelos decretos nº 34.276/2013, nº 35.382/2014 e nº

> 36.690/2015, nos órgãos e entidades da Administração Pública Direta e Indireta do Poder Executivo Distrital. (DISTRITO FEDERAL/DF 2018);
> Instrução Normativa n° 01/2017 – Regulamenta os procedimentos dos serviços de ouvidoria tratados na Lei nº 4.896/2012, Decreto nº 36.462, de 23 de abril de 2015 e estabelece instrumentos de responsabilização dos participantes da rede de ouvidorias e áreas envolvidas. (DISTRITO FEDERAL/DF 2017);
> Instrução Normativa n° 02/2015 – Disciplina a divulgação, nos sítios oficiais na rede mundial de computadores – internet, de informações de interesse geral ou coletivo, custodiadas e produzidas pelos órgãos do Governo do Distrito Federal, observado o disposto na Lei Distrital nº 4.990 de 2012 – LAI/DF. (DISTRITO FEDERAL/DF 2015);

Em complementação às diversas Legislações Pertinentes, no que aduz ao Direito Digital também é respaldo através de Portarias nas quais, são atos administrativos emitidos por autoridades governamentais ou por entidades públicas e privadas com a finalidade de regulamentar os procedimentos nessa esfera, estabelecendo regras específicas para tomadas de decisões administrativas e/ou fornecer orientações sobre essa temática. Isto posto, temos como portarias as seguintes previsões:

> Portaria nº 341/2019 – Determina que todas as denúncias recebidas pelas Ouvidorias dos órgãos do DF devem ser analisadas pelas Unidades de Correição e de Controle Interno. (DISTRITO FEDERAL/DF 2019);
> Portaria nº 342/2019 – regulamenta o Decreto nº 39.723/2019 na caracterização das ocorrências ou situações graves das manifestações recebidas pelo Sistema de Gestão de Ouvidoria do Distrito Federal – SIGO-DF. (DISTRITO FEDERAL/DF 2019);
> Portaria n° 75/2019 – Delega competências ao Ouvidor-Geral do Distrito Federal. (DISTRITO FEDERAL/DF 2019);
> Portaria n° 51/2018 – Institui, no âmbito da Controladoria-Geral do Distrito Federal, o horário de atendimento presencial da Ouvidoria-Geral do Distrito Federal, bem como os procedimentos necessários para garantir a melhor prestação de serviço de ouvidoria. (DISTRITO FEDERAL/DF 2018);
> Portaria n° 21/2017 – Aprova e institui a Agenda Estratégica do Sistema de Gestão de Ouvidorias – SIGO/DF. (DISTRITO FEDERAL/DF 2017);

Por fim, a legislação pertinente é essencial para a organização e regulamentação da sociedade, pois fornece diversas legislações que contemplam o assunto para promover o funcionamento adequado e justo da sociedade.

4 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

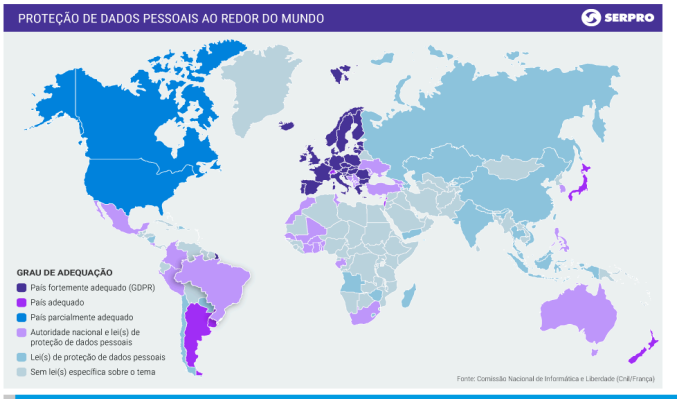
No ano de 1988, na França houve um início de proteção de dados através de uma convenção, da forma como se encontra hoje no Brasil. Tal documento surgiu na época para

proteger os dados pessoais que já estavam transacionando por conta da globalização, com isso, alguns países aderiram a essa convenção. A LGPD surgiu no Brasil em agosto de 2018, no contexto do grande avanço dos meios virtuais e falta de regulação acerca das interações nesse ambiente tecnológico, fato que propiciava um grande número de crimes cibernéticos e fraudes (BRASIL 2018).

De acordo com PIURCOSKY (2019), a população está cada vez mais vulnerável na atual economia digital, principalmente nas redes sociais, ainda, nos cadastros de organizações que agem de maneira virtual. Com isso, é notável que limitar o acesso aos dados pessoais por parte de terceiros irá depender na maioria das vezes do usuário, porém tem aceitável influência para manter a segurança do titular da informação por causa da organização proprietária da rede social.

A Lei Geral de Proteção de Dados (LGPD) n°13.709/2018 é uma modificação que está em concordância com as regras internacionais da atualidade que diz a respeito da proteção de dados (AFFONSO, 2021). Esta lei, tenta unificar os mais de 40 diferentes estatutos que atualmente governam os dados pessoais, online e offline, substituindo certas regulações e suplementando outras. Tal similaridade é compartilhada com o Regulamento Geral sobre a Proteção de Dados (GDPR, sigla em inglês) da União Europeia, um documento do qual serviu de inspiração para a LGPD. Basicamente, a GDPR objetiva proteger o titular do dado pessoal, obrigando os serviços de coleta de dados a informar claramente que o fazem.

MAPA DOS PAÍSES ADEQUADOS A LGPD



Fonte:Comissão Nacional de Informática e Liberdade (C45ni/França)

No Brasil, o foco da LGPD também é a proteção de dados pessoais da pessoa natural, sejam eles sensíveis ou não. A proteção dos dados pessoais tem, como premissa, a defesa da privacidade. Com a privacidade assegurada de maneira apropriada, as liberdades individuais estarão protegidas. Ainda, regulamenta a coleta, armazenamento, tratamento e

compartilhamento de dados pessoais, inclusive em meios digitais, tendo por objetivo trazer mais segurança e privacidade ao indivíduo que cede seus dados pessoais a empresas ou afins. Ela é o instrumento legislativo responsável por resguardar os direitos constitucionais fundamentais a liberdade e privacidade da pessoa natural de direito no que tange a coleta e armazenamento de dados como versa em seu texto (BRASIL, 2018).

4.1 PROTEÇÃO DE DADOS PESSOAIS: FUNDAMENTOS TEÓRICOS E HISTÓRICOS

Segundo o Ministério Público Federal (2023), a LGPD tem por fundamentos principais a segurança e a privacidade e, além disso, ela também assegura a livre iniciativa e a liberdade de expressão do indivíduo de ceder ou não seus dados pessoais, tendo como fator preponderante de tais fundamentos o consentimento do titular dos dados, devendo ser abordado de forma clara e correto, para autorizar, tendo, ainda, a liberdade de aceitar ou não, o uso de suas informações pessoais por parte de terceiros, sejam eles agentes físicos, públicos ou privados.

Os fundamentos encontram-se explícitos no Art. 2 da Lei 13.709/18:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - à inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Outrossim, é importante destacar que há dois tipos de dados que são resguardados pela LGPD, os dados pessoais e os dados pessoais sensíveis, sendo os dados pessoais todo e qualquer dado relacionado a uma pessoa identificada ou identificável, como por exemplo: nome, cadastro de pessoa física (CPF), registro geral (RG), endereço, entre outros.

Já os dados pessoais sensíveis são aqueles capazes de gerar qualquer tipo de desconforto ou constrangimento para o titular caso divulgados, como por exemplo: posição política, orientação sexual, quadro clínico, entre outros.

A fim de inibir o descumprimento da norma pelos agentes de tratamento dos dados, a LGPD dispõe de uma série de ações para atuar e penalizar aqueles que cometerem infrações. Em seu Art. 52 a Lei 13.709/18 expõe o rol de “penalidades impostas a tais infratores,

partindo de advertências e multas, podendo chegar até a proibição parcial e total de funcionamento, tendo a possibilidade de afetar seus negócios de forma significativa.”

> Basicamente, a principal preocupação é com a privacidade das pessoas e o cuidado com a segurança dos dados armazenados. Dessa maneira, a empresa não pode armazenar nenhuma informação que possa identificar um usuário sem o consentimento dele. (BRASIL, 2019).

Diante disso, a Lei nº 13.709 de 14 de agosto de 2018 dispõe sobre a proteção de dados pessoais alterando a Lei nº 12.965, de 23 de abril de 2014 Marco Civil da Internet, propondo cerca de 65 artigos distribuídos em 10 capítulos e com suas respectivas seções. (BRASIL, 2018).

Em contrapartida, a Lei nº 13.853 de 08 de julho de 2019, altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências (BRASIL, 2019).

4.2 CONCEITOS, PRINCÍPIOS E INSTITUTOS DA LGPD. DO TRATAMENTO DE DADOS PESSOAIS E DOS DIREITOS DO TITULAR. DA SEGURANÇA E DAS BOAS PRÁTICAS

A Lei Geral de Proteção de Dados (LGPD), Lei n°13.709/2018, legislação brasileira que regulamenta o tratamento de dados pessoais por organizações públicas ou privadas, é inspirada na GDPR, Regulamento Geral de Proteção de Dados, da União Europeia com o objetivo de proteger a privacidade e os direitos fundamentais das pessoas em relação aos seus dados pessoais.

Com isso, essa legislação possui como norteador seus princípios e conceitos para embasamento jurídico nos seguintes termos:

Tabela 3 - Classificação e conceito dos princípios da LGPD

Finalidade	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
Adequação	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
Necessidade	Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.
Livre acesso	Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.
Qualidade dos dados	Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos

Fonte: Conselho Nacional do Ministério Público

Outrossim, também são classificados os direitos dos titulares para que ao permitir o uso e tratamento de seus dados pessoais, de modo algum e em nenhuma circunstância, seja transferido a outrem a condição de dono de seus próprios dados pessoais. Sendo assim, temos (1) Direito de Acesso, possibilitando ao titular de obter do controlador a confirmação de que seus dados pessoais estão sendo tratados e informações sobre esse tratamento. (2) Direito a correção, onde o titular possa solicitar a correção de dados incompletos, inexatos ou desatualizados. (3) Direito de exclusão (ou "Direito ao esquecimento", podendo o titular solicitar a exclusão de seus dados pessoais, exceto em casos previstos em lei. (4) Direito à portabilidade, facultado ao titular de receber os dados pessoais fornecidos a um controlador, em formato estruturado. (PGE/ES, 2023)

Segundo Get Privacy (2022), site especializado em privacidade, publicado em 2022 a necessidade que as empresas precisam aderir às boas práticas com a segurança dos dados, com isso, temos as seguintes possibilidades: (a) Segurança da informação, implementando medidas para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais. (b) Boas práticas de tratamento, através de adoção de políticas e procedimentos internos que estejam em conformidade com a LGPD. (c) Incorporação de medidas de proteção de dados desde o início do desenvolvimento de sistemas e serviços, também chamado de "Privacy by Design e by Default". (d) Realizar o (RIPD), chamado de Relatório de Impacto à Proteção de Dados, para avaliar o impacto do tratamento de dados pessoais que possam apresentar riscos elevados à privacidade.

Por fim, é através dos institutos da Lei Geral de Proteção de Dados (LGPD), em que desempenham papéis fundamentais na implementação e fiscalização dessa legislação, conforme dispõe a Autoridade Nacional de Proteção de Dados (2023):

- Autoridade Nacional de Proteção de Dados (ANPD), é o órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD no Brasil, tendo como principais atribuições: recebimento de reclamações dos titulares de dados, aplicação de sanções em caso de descumprimento da legislação, elaboração de diretrizes e normas para adequação da LGPD, bem como, também orientar as empresas e cidadãos sobre as melhores práticas em proteção de dados pessoais.

Atuando como autoridade independente, promovendo a proteção dos direitos dos titulares.

- Encarregado DPO - Data Protection Officer, em que um profissional designado pela organização para atuar como intermediário entre o controlador, os titulares de dados e a ANPD, tendo como principais responsabilidades: orientar a empresa sobre as práticas de tratamento de dados pessoais, monitorar o cumprimento da legislação e de políticas internas de proteção de dados, atuar como ponto de contato para os titulares de dados e para ANPD, por fim, colaborar na elaboração de Relatórios de Impacto à Proteção de Dados (RIPD) quando necessário. Exercendo um papel crucial no auxílio à organização para cumprir as obrigações previstas na LGPD. Tendo como obrigatória sua presença em determinadas situações, especialmente quando o tratamento de dados é realizado por entidades de grande porte ou envolve categorias sensíveis de dados.

Em resumo, a ANPD e o Encarregado são peças-chaves no ecossistema da LGPD, contribuindo para a aplicação e fiscalização efetiva da legislação, bem como para o estabelecimento de práticas responsáveis de tratamento de dados por parte das organizações, visando garantir a privacidade e os direitos dos titulares para que sejam protegidos de acordo com os princípios estabelecidos na lei.

4.3 APLICAÇÃO DA LGPD NAS EMPRESAS

Diante desse cenário, fica cabível que as empresas assumam toda a responsabilidade no tratamento, bem como coleta e o armazenamento de dados apresentando como os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade, conhecida com tríade CIA, sendo focado na proteção e privacidade on-line, assim como a liberdade de se expressar e a segurança da informação de pessoas naturais (PEIXOTO, 2020).

A fim de, cumprir o estabelecido pela LGPD, às empresas que tendem a coletar e manipular dados necessita garantir a segurança contra as intimidações de possíveis

vazamentos de locais onde estão armazenados. É relevante que necessite ter cuidados com a segurança da informação nas organizações e que sejam tratados, normalmente, a partir de uma política de segurança interna.

Em contrapartida, FRAZÃO (2018) afirma que esse tipo de situação na maioria das vezes trará impacto direto na vida desses indivíduos, pois terão acesso facilitado/dificultado a crédito, empregos até mesmo serviços e, ainda mencionando da probabilidade de que esses dados contenham informações incompletas/desatualizados.

Nesta perspectiva, faz-se notório que o direito está em constante adaptação aos fatos ocorridos em sociedade, logo, se faz necessária uma evolução legislativa para acompanhar as demandas remanescentes de tais avanços. Por conseguinte, não poderia ser diferente quanto à regulação no armazenamento de dados. Diante dessa assertiva, RAMOS (2021) menciona que o direito essencial à Informação é embasado em três pilares dimensionais: o direito de informar, o direito de se informar e o direito de ser informado.

5 DESAFIOS PARA APLICAÇÃO DA LGPD NAS ORGANIZAÇÕES EMPRESARIAIS

Tendo em vista que a Lei Geral de Proteção de Dados, Lei nº 13.709, foi promulgada no Brasil em 14 de agosto de 2018, passando por um período de “vacatio legis”, ou seja, vacância da lei, no qual passou por etapas, com a maioria de suas disposições entrando em vigor em setembro de 2020, após um período de adaptação, pode-se considerar uma lei muito recente que, por conseguinte ainda não traz um referencial histórico quanto à atuação das empresas em consonância com o referido regulamento e suas complexidades de proteger os dados pessoais dos indivíduos.

Desta forma, existem alguns desafios comuns que as organizações empresariais enfrentam para se enquadrarem dentro das normativas vigentes no país. Passando a buscar consultorias jurídicas para superar tais desafios encontrados através de treinamentos e conscientização para implementar medidas de segurança de dados e procedimentos internos sólidos para garantir a conformidade com a lei.

Segundo estudo disponibilizado pela SERPRO (2021), uma pesquisa feita pela RD Station constatou com uma média de 997 participantes, revela que cerca de 77% dessas

companhias estão atrasadas para implementar a LGPD, estando passíveis de lidar com as punições previstas em lei. Segundo a pesquisa, apenas 7% finalizaram a adequação da LGPD, enquanto 8% ainda estão na etapa final do processo. Sendo assim, cerca de 69% das empresas estão em processos de adequação ou ainda iniciando a construção de uma política própria para a proteção aos dados dos clientes.

Entre as principais barreiras, aponta-se que os fatores para a lentidão da regularização aos padrões da Lei Geral de Proteção de Dados, dar-se-á pela ausência de pessoas especializadas ou de conhecimento na organização, resultando em conflito de quais áreas precisam receber esses cuidados.

De modo geral, existe uma falta de clareza de quais são os próximos passos a serem dados para regularização de acordo com a legislação vigente, resultando em cerca de apenas 3% de companhias que buscam apoio com consultorias especializadas.

5.1 ADAPTAÇÃO DAS EMPRESAS E ORGANIZAÇÕES À LGPD

Em suma, praticamente todas as empresas acabam de forma direta ou indireta, lidando com dados pessoais de terceiros: sejam clientes, fornecedores ou até mesmo o de concorrentes. Desta forma, é imprescindível atentar-se às regras da Lei Geral de Proteção de Dados.

No entanto, a implementação da LGPD pode não ser muito complicada para empresa quando esta opta por buscar métodos externos para regularização empresarial através de assessorias especializadas no assunto. Mas, para isso é necessário que a empresa garanta a segurança plena de todas as informações e para isso ser possível, é indispensável um sistema de proteção de dados que garanta a segurança do comprometimento da gestão dos dados, como também, automatize e otimize diversos processos, permitindo maior controle de todas as etapas de processos na empresa.

Apesar de ainda gerar confusão e dúvidas por parte de empresas e usuários, a lei foi instaurada para reforçar a proteção, permitindo a um indivíduo o acesso, verificação e, até mesmo, a eliminação das suas informações de todos os negócios ou instituições públicas, caso queira. Em outras palavras, pontua, basicamente, que todo dado precisa ser solicitado para uma finalidade específica, devendo ser resguardado contra vazamentos e fraudes.

É indubitável que para as grandes empresas como multinacionais, empresas de capital aberto e empresas de grande porte em geral, o processo adaptativo vem sendo mais fácil, tendo algumas dessas empresas até mesmo se antecipado após a publicação da Lei para se adequarem às exigências trazidas pela norma, uma vez que elas em sua maioria dispõem de recursos, um setor jurídico para acessória e demandas em geral e um sistema organizacional distinto quanto a sua estruturação.

Ademais, temos no sentido oposto às micro e pequenas empresas, que por sua vez dispõem de recursos muito mais limitados, uma estruturação na maior parte das vezes concentrada, onde uma única pessoa acaba cumulando responsabilidade por mais de uma frente da empresa (administração, RH, etc.), onde a adaptação a lei se torna muito mais desafiadora. Não obstante, em consonância com a maior dificuldade dos agentes de pequeno porte e com o objetivo de trazer paridade e isonomia à adequação dos agentes, a Autoridade Nacional de Proteção de Dados (ANPD), no dia 27 de janeiro de 2022, publicou a RESOLUÇÃO CD/ANPD N° 2 que especificou em seu texto quem são os agentes de pequeno porte e resguardou para eles um tratamento diferenciado quanto à aplicação da lei 13.709/2018, em pontos como os prazos, registro das operações de tratamento, as comunicações dos incidentes de segurança, o encarregado pelo tratamento de dados pessoais e a segurança e boas práticas.

> Art. 9º Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, de forma simplificada.
> Art. 10. A ANPD disporá sobre flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da regulamentação específica.
> Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD.
> Art. 13. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> Art. 14. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro:
> I - no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais, conforme previsto no art. 18, §§ 3º e 5º da LGPD, nos termos de regulamentação específica;
> II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, nos termos de regulamentação específica, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento, conforme os termos da mencionada regulamentação;
> III - no fornecimento de declaração clara e completa, prevista no art. 19, II da LGPD; IV - em relação aos prazos estabelecidos nos normativos próprios para a

> apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento. (BRASIL, 2022)

Conforme supracitado da lei e para haver harmonia entre o prestador do serviço e ao favorecido por esse, é relevante que tenham conhecimento sobre cada artigo mencionado, principalmente para as empresas de pequeno porte e assim permanecer o controle sobre os dados de seus clientes.

5.1.1 Desafios técnicos e operacionais para a implementação da LGPD

No que tange a LGPD nos dias atuais, é possível apontar como principal desafio a criação de uma cultura de proteção de dados, uma vez que historicamente é enraizada na sociedade brasileira a cultura da publicidade dos dados.

Aliado a isto, atualmente as empresas coletam de maneira demasiada os dados de seus consumidores, sem nenhum tipo de restrição ou regulação, dos dados de seus consumidores acerca de cada usuário que utiliza plataformas online, redes sociais entre outros, nas quais as pessoas compartilham dado de maneira pública frequentemente, normalizando a disposição de dados pessoais no decurso do tempo. Portanto não basta a implementação de uma norma regulamentadora, apesar da norma ser necessária, ela é apenas o começo, se faz necessário a sensibilização da importância do tratamento de dados desde o cedente dos mesmos.

> “Sabemos que há empresas com um nível de aculturamento maior, e que há outras que focam numa ‘imagem’ de cultura de privacidade de dados que, na verdade, não se espelha nem nas suas políticas e muito menos no seu cotidiano. Cultura de privacidade, de fato, é dia a dia, realidade, é você educar por exemplos. (COTS, 2020).

O advogado COTS (2020), “afirma que com essa a lei, digamos que “nova” será permitido uma visão diferenciada para novos paradigmas, pois, mesmo com a existência de leis que já atuam nesse certame, a LGPD cria um “ordenamento para regular a matéria, e não só para complementar algo existente” assegura o COTS, 2020.

Com isso, muitas organizações precisam promover a conscientização e educar seus funcionários sobre a importância da LGPD e as práticas adequadas de proteção de dados.(grifo nosso)

Sobretudo, as empresas precisam revisar e ajustar seus processos internos para garantir que estejam em conformidade com os requisitos da LGPD, o que pode envolver a criação de novos procedimentos e políticas e que muitas das vezes, é um desafio para organização. Tal procedimento é de suma relevância, uma vez que a LGPD exige que as organizações obtenham o consentimento adequado para coletar e processar dados pessoais. Isso pode ser desafiador, pois requer transparência e documentação adequada.

Diante disso, em consonância com o Art. 7, §5, 2018, da Lei Geral de Proteção de Dados, temos:

> Art. 7° O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento do consentimento pelo titular;
> § 5° O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei. (BRASIL, 2018)

Sendo assim, conforme recomendação da GET PRIVACY (2023) mapear os dados pessoais é o primeiro passo para a adequação a nova legislação, tendo em vista que é por meio dele que a empresa vai mapear toda a rota dos dados pessoais de seus clientes, colaboradores e fornecedores percorrem dentro da corporação, pontuando desde quais são os dados coletados no ato do atendimento, qual a necessidade deles para a prestação do serviço, como e onde serão armazenados, por quais setores da empresa esses dados irão passar, bem como o tipo de tratamento de cada setor terá acerca deles, com quem eles serão compartilhados e por quanto tempo irão permanecer no banco de dados da empresa, isso implica em implementar medidas robustas de segurança de dados para proteger as informações pessoais e evitar vazamentos ou violações de dados.

Por ser uma norma recente, ainda não há um padrão quanto a realização do procedimento, com isso, para maior facilidade a LGPD prevê a obrigatoriedade que as organizações designar um Encarregado de Proteção de Dados (DPO), conforme Art. 41 da Lei Geral de Proteção de dados Lei n°13.853/19, para que estes assumam a responsabilidade pela proteção dos dados. Isso pode ser um desafio, pois envolve a prestação de contas. Por isso, as

organizações devem estar preparadas para lidar com solicitações de titulares de dados, como acesso, retificação, exclusão e portabilidade de dados, dentro dos prazos especificados na lei.

Dito isso, cabe às empresas estabelecer processos de monitoramento e auditoria para garantir a conformidade contínua com a LGPD e documentar as atividades de processamento de dados, para manter a transparência sobre como estão coletando, processando e armazenando dados pessoais e comunicando claramente essas práticas aos titulares de dados.

Por fim, dentre o que pode representar um desafio para algumas empresas para a implementação da LGPD está o investimento em tecnologia, pessoal e treinamento, com isso, o valor financeiro pode ser considerado como um dos maiores desafios no decorrer dessa regularização (DAMÁSIO, 2023). Entretanto, a LGPD prevê a aplicação de multas significativas em caso de não conformidade, o que aumenta a pressão sobre as organizações para cumprir a lei.

5.2 CONTRATOS EMPRESARIAIS: ADEQUAÇÕES

Segundo LIMA, Adrianne (pg. 9, 2021) ao analisar as relações contratuais, a expressão “relação” traz um significado à conexão existente entre uma coisa e outra. Significa um vínculo contratual advindo de um acordo de duas ou mais vontades, nos termos da ordem jurídica destinado a estabelecer e reger uma regulamentação de interesses entre as partes.

O contrato, por sua vez, é a materialização de um negócio jurídico, ou seja, é a manifestação de vontade com a intenção de gerar efeitos jurídicos, constituindo um negócio jurídico. (LIMA, Adrianne, 2021, pg. 9)

O Código Civil, é um norteador de interpretação jurídica nas relações contratuais que envolvem a proteção de dados pessoais (LIMA, Adrianne, 2021, pg. 9), que por sua vez, ao interpretar e elaborar um contrato com as normas de proteção de dados é imprescindível incluir as previsões da LGPD, bem como, cumprir os requisitos das normas gerais de contratos uma vez que são as mesmas para todos os negócios jurídicos.

Além disso, toda vontade é acompanhada de uma responsabilidade na atuação do contratante e contratado, derivada da hierarquia das normas superiores como a Constituição

da República bem como, embasado e acompanhado de outras normas dispersas em outros Códigos.(LIMA, Adrianne, 2021, pg. 9)

A Lei Geral de Proteção de Dados está altamente ligada com o tema contratos, isso porque todas as pessoas, sejam físicas ou jurídicas, que possuam contratos firmados em que compartilhem dados sensíveis como Nome, E-mail, Telefone entre outros, precisam adequar-se para conter as previsões de cláusulas de proteção de dados, de acordo com a conformidade da LGPD nos quais envolvam a forma do tratamento dos dados pessoais. (LIMA, Adrianne, 2021, pg. 9)

O alcance desta normativa, dialoga com outras já existentes anteriormente, isso se dá devido a certas lacunas que ainda existem nessa nova legislação. Com isso, é de suma importância que ao interpretar esta lei seja analisada conjuntamente com demais leis pertinentes ao assunto devido a carência de interpretação da normativa no qual necessita da contribuição de demais dispositivos positivados em outras legislações. Um exemplo desse caso, é ao analisar um contrato de trabalho lidamos com dados sensíveis. Uma vez que a Lei Geral de Proteção de Dados não possui previsão específica para essa matéria legislativa, para atingir seu ápice de interpretação o contratante deverá utilizar como apoio a CLT (Consolidação das Leis do Trabalho) e a Constituição Federal. (LIMA, Adrianne, 2021, pg. 9)

Um dos requisitos imprescindíveis de um contrato refere-se ao seu objeto. O objeto do contrato deve ser lícito, não podendo contrariar a lei ou os bons costumes, como por exemplo, não pode haver um contrato de contrabando uma vez que contradiz o que está disposto em lei. Outro ponto também, o objeto do contrato deve ser possível, ou seja, a possibilidade deve ser tanto física como jurídica, pois a impossibilidade jurídica encontra obstáculo no ordenamento, como por exemplo, a contratação de um menor de idade, por lei, não se pode exercer trabalho de CLT com uma jornada de 8 (oito) horas menor de 18 (dezoito anos). (LIMA, Adrianne, 2021, pg. 9)

Em suma, os encarregados pelos Tratamentos de Dados Pessoais devem agir em conformidade com a Política de Segurança de Privacidade do contratante, ou seja, o contratado deverá respeitar não somente o previsto em contrato, manuais ou códigos, mas sim, o que há estabelecido como segurança jurídica por parte do contratante. (LLIMA, Adrianne, 2021, pg. 9)

5.2.1 Função social do contrato

A função social do contrato é uma norma importante aos contratos que vem enunciada já no primeiro artigo do Código Civil que inaugura as disposições sobre os contratos em geral, conforme o art. 421 “A liberdade contratual será exercida nos limites da função social do contrato”. (BRASIL, 2018).

Na mesma previsão, a lei preceitua que os contratos podem ser elaborados com total autonomia das partes de acordo com os seus interesses, mas que essa autonomia fica limitada pelo interesse social, também chamado por Sílvio Venosa como “freio da função social” (VENOSA, Sílvio de Salvo. Atlas, 2016, v. II), ou seja, se violados tais limites poderão as partes recorrer ao sistema judiciário.

Contudo, por mais que a lei predisponha limites para função social, esse conceito ainda é bastante aberto e indeterminado, sendo difícil fornecer uma definição teórica. Conforme aponta Pablo Stolze e Rodolfo Pamplona Filho: “Sem pretendermos exaurir esforços na hercúlea tarefa de definir a função social do contrato, ela poderá, por outro lado, ser delimitada no espaço jurídico de atuação em que se projeta”. (GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo, p. 398)

Dessa forma, devemos nos perguntar como a função social do contrato seria atingida na temática de proteção de dados pessoais.

No entanto, considerando que a Lei Geral de Proteção de Dados foi criada devido a uma demanda social, no qual um conjunto de situações que ocorriam e não possuíam um amparo legal adequado referente ao tratamento de dados pessoais de titulares, bem como por ser de caráter específico na legislação, de fato faz se como concluinte que a função social do contrato, no que tange a LGPD será cumprida quando observada e aplicada a Lei 13.709/2018 e quando necessário a complementação da aplicação de outras leis.

De modo geral, para concretizar a observância à função social do contrato frente a proteção de dados, é necessário adicionar e rever cláusulas do contrato para adequação perante a lei, outrossim, no próprio dispositivo legal aduz em suas normativas seus princípios, os quais dispõe de um manual de como atingir e observar a função social do contrato, no que diz respeito à proteção de dados de terceiros.

De modo a tornar mais claro o limite e lograr com êxito o cumprimento da função social em um contrato, além das normativas previstas na Lei Geral de Proteção de Dados, temos como fundamento predispostos em outras legislações vigentes nos artigos 421 do Código Civil; Art. 1°, III, art. 3°, I, art. 5°, caput, XXII e XXIII, art. 170°, III, previstos pela Constituição Federal. (BRASIL, 2018)

5.2.2 Princípios basilares e elementos essenciais de uma relação contratual

Os princípios são os verdadeiros "nortes" de interpretação da norma. Tem como valor social a partir do momento em que surge e amadurece na sociedade, passando a ganhar maior relevância. Na mesma medida em que o princípio pode deixar de ser aceito na sociedade.

Conforme o ilustre REALE, Miguel (Filosofia do direito, p.60): "Princípios são, pois verdades ou juízos fundamentais, que servem de alicerce ou de garantia de certeza a um conjunto de juízos, ordenados em um sistema de conceitos relativos à dada porção da realidade".

Os princípios passam a ser vetores interpretativos e mestras de todas as demais normas presentes, uma vez que, norteiam as situações do cotidiano, embora não materializadas em um dispositivo, estão protegidas indiretamente por princípios.

Além dos princípios da Lei de Proteção de Dados, também é necessário analisar os Princípios Gerais dos Contratos, os quais são: (a) autonomia da vontade, em que está materializada na liberdade de estabelecer uma relação jurídica contratual; (b) força obrigatória dos contratos, em que possui o significado que o contrato válido e eficaz deve ser cumprido pelas partes (pacta sunt servanda). (c) relatividade dos contratos, que tem por base o fundamento de que os terceiros não envolvidos em uma relação contratual, não estão submetidos ao efeito deste contrato; (d) princípio da boa-fé nos contratos, atrelada ao dever das partes de agir de forma correta, eticamente, em todas as fases dos contratos, isto porque, mesmo após seu cumprimento, podem lhe sobrar efeitos residuais, destacado por (LIMA, Adrianne, 2021, pg. 11)

Outro fator existe na relação contratual são os elementos essenciais do negócio jurídico, podendo ser encontrados no Código Civil, especificamente no artigo 104° em que dispõe que os elementos essenciais são: agente capaz, objeto lícito e forma prescrita ou não proibida pela lei, tais elementos são prismas dos negócios jurídicos podendo serem nulos os contratos que faltar qualquer dos elementos essenciais.

Cada contrato, específico da sua natureza possuem elementos essenciais, como por exemplo um contrato de compra e venda possui os elementos específicos: a coisa, o preço e o consentimento), com isso, ao elaborar um contrato faz-se necessário observar a Lei Geral de Proteção de dados em suas bases legais, princípios e as regras de responsabilidades estabelecidas por lei.

5.2.3 Responsabilidade civil na LGPD: subjetiva ou objetiva?

No tocante às cláusulas gerais da responsabilidade, o direito e, em especial, o direito das obrigações impõe deveres de conduta. Esses deveres resultam de um dever geral de conduta, o qual o Direito e os bons costumes impõem, sendo um deles o cumprimento contratual sob pena de responsabilização.

No que diz respeito acerca da diferença acerca das definições sobre a responsabilidade civil objetiva e responsabilidade civil subjetiva, a ilustre LIMA, Adrianne (2021, pg. 12) dispõe:

RESP. CIVIL OBJETIVA	RESP. CIVIL SUBJETIVA
Independe da prova de **culpa**; há verdadeira presunção *de* culpabilidade do agente.	**Depende** da prova de **culpa** ou dolo do agente que praticou o ato.

Com previsão nos dispositivos da Lei Geral de Proteção de Dados Pessoais (LGPD) tratou o tema na Seção III, nos artigos 42 e 43, instituindo regras para algumas responsabilidades como: reparação de dano patrimonial, moral, individual ou coletivo, sendo estes praticados por controladores ou operadores.

No entanto, o legislador foi omisso sobre qual seria a teoria adequada para a responsabilização daqueles que violarem as normas de proteção de dados, com isso, a interpretação deve ser feita através de uma análise jurídica, histórica e principiológica.

Conforme dispositivo da Lei Geral de Proteção de Dados N°13.853/2019, em seu artigo 42 aduz:

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
> § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
> I – O operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
> II – Os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.
> § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.
> § 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.
> § 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso. (BRASIL, 2018)

No art. 42 o legislador a responsabilidade dos envolvidos nas operações de tratamento de dados pessoais, deixando de forma explícita a possibilidade da reparação dos danos patrimoniais, moral, individual e coletivo. A LGPD, inclina-se para a responsabilidade civil de ordem subjetiva, uma vez que não há menção de risco de prova. O artigo 43, por sua vez, traz hipóteses de excludentes de responsabilidades:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I – Que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II – Que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros.
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros. (BRASIL, 2018)

O inciso III supramencionado, demonstra que a indicação do culpado, é um fato indispensável para a caracterização do dano. Contudo, a própria lei não dispõe expressamente qual seria a responsabilidade de tal ação, sendo assim, enquanto a Autoridade Nacional de Proteção de Dados (ANPD) não regulamentar tal aplicação, caberá ao operador de direito utilizar como ferramenta a hermenêutica jurídica para compreensão legal.

Outrossim, a Lei Geral de Proteção de Dados Pessoais aduz também acerca da responsabilidade solidária do operador ao controlador, nos seus artigos 42 e 43, sendo responsabilidade solidária caracterizada quando o operador descumpre a lei, ou age em desacordo com as ordens do controlador (inciso I do § 1° do art. 42). Bem como, também responde com responsabilidade solidária entre os controladores quando estes estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados, salvo nos casos de exclusão previstos no art. 43 (inciso II do §1° do art. 42). Por isso, incube as partes (controlador e operador) ter expressamente em contrato de maneira explícita e inequívoca o tratamento a ser realizado. (BRASIL, 2018)

5.3 EXTINÇÃO DO CONTRATO

O termo “extinção” , também chamado de “dissolução” ou “rescisão” do contrato, são termos equivalentes, previstos no Código Civil, no capítulo II do Título V, “Dos Contratos em Geral”.

A extinção do contrato pode ocorrer de forma normal, por vontade das partes quando as partes estão ou não satisfeitas com o cumprimento do que foi pactuado. Bem como, poderá ter a sua extinção de forma “natural”, sendo dissolvida pela verificação de uma circunstância prevista pelas partes e tida como “esperada”. O regular cumprimento do contrato, não se limita a ela, uma vez que, por força de disciplina normativa do negócio jurídico, podem as partes estabelecer elementos de eficácia em que se limitam na produção de efeitos do contrato, possibilitando sua extinção. (BARONOVSKY, Thainá, 2021, pg. 13).

As partes, podem celebrar um contrato sem pré fixar um prazo de finalização, tendo como exemplo os contratos de renovação automática, em contrapartida no âmbito trabalhista temos como exemplo os contratos empregatícios que são baseados no princípio da continuidade da relação do emprego, dentre outros, tendo como regra, a concessão de um aviso prévio.

Contudo, um contrato na esfera de proteção de dados, mais uma vez, o legislador não tratou sobre esse tema especificamente na Lei Geral de Proteção de Dados Pessoais, tendo que ser observadas todas as regras do Código Civil.

5.3.1 Consequências jurídicas em caso de descumprimento da LGPD

Dentre as principais consequências do não cumprimento da LGPD, é o risco de sanções administrativas, conforme Art. 52 da Lei n°13.709 de 14 de Agosto de 2018:

> 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: (Vigência)
> 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; (BRASIL, 2018)

Tendo como órgão regulamentador de fiscalização do cumprimento da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD), de acordo com o previsto em lei.

Outra consequência do descumprimento da LGPD é o risco de perda de confiança. Em um mundo cada vez mais conectado e digital, a privacidade e a segurança dos dados pessoais são temas sensíveis e que preocupam os consumidores. Uma empresa que não se preocupa com a privacidade e a segurança dos dados pessoais de seus clientes pode acabar perdendo a confiança do público e, consequentemente, a sua autoridade. (DE SÁ, Bruna, 2023).

De SÁ, Bruna (2023) também elucida danos financeiros sendo uma das consequências resultantes do descumprimento da LGPD para as empresas. Isso ocorre porque a LGPD prevê que os titulares dos dados pessoais têm direito a receber uma indenização por danos morais e materiais decorrentes do tratamento inadequado de seus dados pessoais.

5.3.2 Multas contratuais vs. Multas administrativas da ANPD

Multas contratuais e multas administrativas são dois tipos de penalidades que podem ser aplicadas em diferentes contextos, principalmente quando se trata de questões regulatórias do âmbito jurídico.

A multa contratual é realizada na elaboração do contrato entre as partes, seja um contrato de prestação de serviços entre outros. Um contrato pode ter a previsão de aplicação de multa por infração à LGPD e nesse caso, há uma definição bilateral onde que ambas as partes consentem com a atribuição da multa, pois este, pode gerar risco financeiro ou reputacional ao controlador. (MONTES, Damarys, 2021, pg. 69).

As multas acordadas entre as partes, possuem um percentual indicado com base no faturamento mensal ou anual, podendo ainda, ter uma indicação de indenização ajustado pelas partes através de negociação e ainda provisionamento do risco e incidentes de dados.

Quando fala-se de multas administrativas, as quais competem aos órgãos do estado, no que se refere às aplicadas pela ANPD (Autoridade Nacional de Proteção de Dados), esta é uma multa prevista no art. 5, II e III da Lei Geral de Proteção de Dados Pessoais. (BRASIL, 2018)

Multas nas quais o caráter seja o descumprimento da legislação vigente, serão aplicadas para quaisquer infrações cometidas, exclusivamente serão aplicadas pela ANPD. Atualmente, as penalidades podem ser aplicadas chegando ao valor de quinhentos milhões de reais ou 2% do faturamento total da empresa. (MONTES, Damarys, 2021, pg. 69).

Assim, existem duas possibilidades de aplicação das penalidades contratuais sendo estas, diante de um acidente de dados pela controladora poderá ser aplicado a multa prevista em cláusulas de caráter indenizatório financeiro e reputacional, assim como pelo órgão regulador, a ANPD, diante da apuração das infrações. (MONTES, Damarys, 2021, pg. 69).

Contudo, as penalidades possuem viés diferenciado e são aplicadas por conceitos diferentes, pôr a primeira refere-se a uma previsão contratual estabelecida e acordada pelas partes e a segunda é decorrente de apuração do órgão responsável. Com isso, a violação ou incidente de dados pode ocasionar às organizações uma perda considerável no cenário financeiro e uma publicização da imagem resultando em falta de credibilidade e reputação da empresa, podendo inviabilizar negócios futuros. (MONTES, Damarys, 2021, pg. 69).

A publicização do incidente ocorrido e os meios para mitigação, com a finalidade de minimizar riscos possíveis aos titulares de dados, é ponto obrigatório preceituado pela LGPD, com respaldo no art. 52, IV da Lei 13.709/18. (BRASIL, 2018).

Portanto, cumpre esclarecer que ambas as multas mencionadas são devidamente legais e podem ser cobradas, tanto pela parte lesada quanto pela ANPD, órgão regulamentador.

CONSIDERAÇÕES FINAIS

Nesse contexto, surge o seguinte questionamento: A conscientização governamental das empresas dialoga na implementação da Lei 13.709/2018? Como fica a estruturação no quesito empresarial?

Diante do exposto neste trabalho pode-se afirmar que com o avanço da internet nos últimos anos é perceptível de enormes conquistas para democratizar a informação.

Em virtude disso, houve também o surgimento de outros desafios no âmbito jurídico no intuito de garantir que o espaço virtual também possa transmitir segurança, havendo sempre as relações entre consumidores e fornecedores de maneira compensada e justa, estabelecendo direitos e deveres e devidamente fazendo menção às normas nacionalizadas.

Devido ao aumento da transação de dados e a temática sobre a segurança e o sigilo destes nos últimos tempos, faz-se necessária a criação de uma lei que necessite regulamentar a maneira de proteger os dados que são gerados em uma rede mundial de computadores, com isso, a LGPD tomou por base a GDPR, lei que é utilizada em países da União Europeia.

Desse modo, com a criação dessa lei as empresas no Brasil, tiveram que se readequar aos moldes da legislação, para que não sofram as consequências dispostas pela LGPD.

Tendo em vista que, o novo não é fácil de adaptar, mas que é preciso para haver maior sigilo aos dados armazenados dos clientes em todas as esferas, sejam físicas ou onlines, tal legislação vem por meio do poder jurídico tomar força resguardando a sociedade, num contexto geral tratando desse assunto para que forneça insumos as empresas para adequarem a estruturação empresarial nos moldes previstos em lei.

Por fim, é notável que a nova lei trouxe impactos sobre tais alterações nas empresas, com isso, passou a ser essencial a prevalência da ética no tratamento e assim, trouxe maior

segurança a todos que compartilham seus dados de alguma forma, em um mundo que está constantemente evoluindo para o ambiente digital.

REFERÊNCIAS

ARAÚJO, Marcelo Barreto de. Comércio eletrônico; **Marco Civil da Internet; Direito Digital.** Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviço e Turismo, 2017.

ASCENSÃO, José de Oliveira. Direito autoral. Rio de Janeiro: Renovar, 1997.

BRASIL, Agência. **Entenda o que é neutralidade de rede e como é o seu funcionamento no Brasil.** Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2017-12/entenda-o-que-e-neutralidade-de-rede-e-como-e-o-seu-funcionamento-no-brasil> Acesso em: 17 nov.2023

BRASIL. **Constituição Federal de 1988.** Disponível em: https://www.jusbrasil.com.br/topicos/10729747/inciso-xxxiii-do-artigo-5-da-constituicao-federal-de-1988. Acesso em: 08 nov. 2023.

BRASIL. **Secretaria de Ciência, Tecnologia e Inovação. Legislação Pertinente**. Brasília. 19 out. 2022. Disponível em: https://www.secti.df.gov.br/legislacao-pertinente/. Acesso em: 6 nov. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União 15 de agosto de 2018. Brasília, DF. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 07 nov. 2023.

BRASIL. Ministério dos Transporte. Departamento Nacional de Infraestrutura de Transportes. **Cartilha da Lei Geral de Proteção de Dados Pessoais – LGPD – 2021.- DINT** Disponível em: https://www.gov.br/dnit/pt-br/acesso-a-informacao/protecao-de-dados-pessoais-lgpd/cartilha_lgpd_2021.pdf Acesso em: 07 nov. 2023.

BRASIL. **LEI Nº 13.853, DE 8 DE JULHO DE 2019**.Diário Oficial de União de 20 de dezembro de 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20192022/2019/Lei/L13853.htm#art2 Acesso em: 08 nov. 2023.

BRASIL. Ministério da Fazenda. SERPO. **Como incentivar um comportamento em prol da proteção de dados?** 2020. COTS, Márcio Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/cultura-privacidade-lgpd-governanca. Acesso em: 08 nov. 2023.

BRASIL. Ministério Público. Conselho Nacional do Ministério Público. Lei Geral de Proteção de Dados Pessoais (LGPD). **Fundamentos e Princípios.** Disponível em: https://www.cnmp.mp.br/portal/transparencia/lei-geral-de-protecao-de-dados-pessoais-lgpd/a-lgpd/fundamentos-e-principios Acesso em: 10 nov. 2023

BRASIL. GOVERNO FEDERAL. Serpro e LGPD. **LGPD: a versão brasileira do regulamento europeu**., 12 set. 2019. Disponível em: https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais Acesso em: 10 nov. 2023

BRASIL. GOVERNO FEDERAL. Serpro e LGPD**. Em que "estágio" estamos? Confira o mapa da proteção de dados pessoais no mundo**: Disponível em: https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais. Acesso em: 10 nov.2023

DAMÁSIO. **LGPD: quais os desafios enfrentados pelo Brasil na sua aplicação.** Disponível em: https://matriculas.damasio.com.br/blog/lgpd-quais-os-desafios-enfrentados-pelo-brasil-na-sua-aplicacao/#:~:text=Falta%20de%20recursos%20e%20capacita%C3%A7%C3%A3o,todas%20as%20exig%C3%AAncias%20da%20lei. Acesso em: 15 nov.2023

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Manual de direito civil: volume único.** São Paulo: Saraiva, 2017, p. 398.

HSC. **By HSC Brasil**. O que é GDPR e o que muda para as empresas e os brasileiros? Disponível em: https://www.hscbrasil.com.br/gdpr/. Acesso em: 07 nov. 2023.

IBM. **O que é armazenamento de dados?** Disponível em https://www.ibm.com/br-pt/topics/data-storage#:~:text=Entre%20os%20dispositivos%20DAS%20temos,de%20estado%20s%C3%B3lido%20(SSD). Acesso em: 17 nov.2023

IPSWITCH, Formely Progress. **Privacidade de dados vs. Proteção de Dados.** Disponível em <https://www.ipswitch.com/pt/blog/privacidade-de-dados-vs-protecao-de-dados> Acesso em: 17 nov.2023

KAMINSKI, Omar. **Introdução à gestão de direitos digitais.** In: WACHOWICZ, Marcos (coord.). Propriedade Intelectual & Internet. Curitiba: Juruá, 2000.

LIMA, Adrianne; SAMANIEGO, Daniela; BARONOSVKY, Thainá. **LGPD para contratos: adequando contratos e documentos à Lei Geral de Proteção de Dados.**

Editora Saraiva, 2021. *E-book.* ISBN 9786555597684. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555597684/. Acesso em: 10 nov. 2023.

PGE/ES. Procuradoria Geral do Estado do Espírito Santo. **Dos direitos dos titulares de dados conferidos pela LGPD.** Disponível em https://pge.es.gov.br/dos-direitos-dos-titulares-de-dados-conferidos-pela-lgpd. Acesso em: 15 nov. 2023.

PRIVACY, Get. **LGPD: confira 10 boas práticas de proteção de dados e privacidade.** Disponível em https://getprivacy.com.br/mapeamento-de-dados-lgpd/#:~:text=Fazer%20o%20mapeamento%20de%20dados%20%C3%A9%20o%20primeiro%20e%20mais,e%20das%20rotinas%20da%20empresa.Acesso em: 15 nov. 2023.

PRIVACY, Get.. **Mapeamento de dados: o que é e qual sua importância na LGPD.** Disponível em: https://getprivacy.com.br/lgpd-boas-praticas Acesso em: 15 nov. 2023.

PINHEIRO, Patricia Peck. Direito digital. 2. ed. São Paulo: Saraiva, 2008.

PLANALTO. **Lei n°12.527, De 18 DE NOVEMBRO DE 2011.** Disponível em <https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm>. Acesso em: 17 nov.2023

REALE, Miguel. **Filosofia do direito.** 11. ed. São Paulo: Saraiva, 1986, p 60

REIS, Maria Helena Junqueira. Computer crimes: a criminalidade na era dos computadores. Belo Horizonte: Del Rey, 1997.

SARAIVA, Editora. **Lei geral de proteção de dados (LGPD) e marco civil da internet**. Editores. Fabiana Dias da Rocha, et al. Editora Saraiva, 2022. *E-book.* ISBN 9786553620384. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620384/. Acesso em: 10 nov. 2023.

STEFANINI GROUP**. Qual é a relação existente entre a indústria 4.0 e a sociedade 5.0?** 14 abr. 2022. Disponível em: https://stefanini.com/pt-br/insights/artigos/industria-4-0-e-a-sociedade-5-0 Acesso em: 6 nov. 2023.

SÁ, Bruna de. **Quais são as consequências de não cumprir a LGPD?,** Jusbrasil. Disponível em: https://www.jusbrasil.com.br/artigos/quais-sao-as-consequencias-de-nao-cumprir-a-lgpd/1833570683#:~:text=Uma%20das%20principais%20consequ%C3%AAncias%20do,R%24%2050%20milh%C3%B5es%20por%20infra%C3%A7%C3%A3o.. Acesso em: 15 nov. 2023.

SCIELO. **A lei geral de proteção de dados em empresas brasileiras: uma análise de múltiplos casos.** PIURCOSKY, Fabrício Peloso; COSTA, Marcelo Aparecido; FROGERI, Rodrigo Franklin; CALEGARI, Cristina Lelis Leal. Versão impressa ISSN 2215-910X Versão online ISSN 2027-5692. Disponível em:

http://www.scielo.org.co/scielo.php?script=sci_abstract&pid=S2215-910X2019000300089&lng=en&nrm=iso&tlng=pt Acesso: 07 nov. 2023.

SILVA, Louise S. H. Thomaz da; SOUTO, Fernanda R.; OLIVEIRA, Karoline F. **Direito Digital.** Editora Saraiva, 2021. E-book ISBN 9786556902814. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786556902814/. Acesso em: 15 nov. 2023.

TEIXEIRA, Ilderlandio. **LGPD e a liberdade de expressão na internet.** Disponível em: https://www.jusbrasil.com.br/artigos/lgpd-e-a-liberdade-de-expressao-na-internet/932956784. Acesso em: 17 nov.2023.

TJDFT. **Responsabilidade do provedor pelo conteúdo publicado em redes sociais.** Disponivel em: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/cdc-na-visao-do-tjdft-1/o-consumidor-na-internet/responsabilidade-do-provedor-pelo-conteudo-publicado-nas-redes-sociais. Acesso em: 17 nov.2023.

TRUZZI, Gisele. PALOTTA, Iasmin. **DIREITO DIGITAL: Tudo o que você precisa saber.** Disponível em: https://techcompliance.org/direito-digital/. Acesso em: 17 nov.2023.

VENOSA, Sílvio de Salvo. **Direito civil: teoria geral das obrigações e teoria geral dos contratos.** 16. ed. rev. e atual. São Paulo: Atlas, 2016, v. II.