



Direito em Revista

NÚMERO 37/2024



Direito em Revista

NÚMERO 37 / 2024

CESUL - CENTRO DE ENSINO SUPERIOR CESUL

Rua Antônio de Paiva Cantelmo, 1222 – Centro
CEP. 85.601-270. Francisco Beltrão – Paraná – Brasil
(46) 3524-4242 / cesul@cesul.br / npic@cesul.br / www.cesul.br

Diretor Geral
Névio Urio

Diretora
Prof(a). Me. Daniela Urio Mujahed

Coordenador do curso de Direito
Prof. Luiz Carlos Dagostini Junior

Editor-Chefe:
Prof. Dr. Gustavo Ellwanger Calovi (CESUL)

Editores Executivos
Amanda Kriger (CESUL)
Profª. Drª Alexia A. Rodrigues Brotto Cessetti (CESUL)
Prof. Me. Bruno Fernandes de Oliveira (CESUL)
Profª Ma. Camila Cararo Tonkelski (CESUL)
Prof. Me. Douglas Balduino Pereira (CESUL)
Prof. Dr. Kenny Sontag (CESUL)
Prof. Me. Lucas Bernardon (CESUL)
Prof. Dr. Luiz Fernando Coelho (CESUL)
Prof. Dr. Marcos Augusto Maliska (CESUL)

Ficha Catalográfica

C421 CESUL- Centro de Ensino Superior
Direito em revista: revista jurídica do centro de ensino superior cesul nº 37. Prof. Dr. Gustavo Ellwanger Calovi. (Coord.), Francisco Beltrão, 2024.

Inclui Bibliografia:
ISSN: 1676-0700

I. Direito em Revista II. Luso-Brasileira
III. Adolescente em Conflito IV. Desinformação

CDD: 340

Ficha Catalográfica elaborada pela bibliotecária Elisandra Artus Berté - CRB-9/1675

CONSELHO EDITORIAL

Prof. Dr. Alfredo de Jesus Dal Molin Flores
Universidade Federal do Rio Grande do Sul, Brasil

Prof. Dr. Anderson Vichinkeski Teixeira
Universidade do Vale do Rio dos Sinos, Brasil

Profª. Drª. Andrea Pitasi
Università degli Studi G. d'Annunzio, Chieti–Pescara, Itália

Prof. Dr. Augusto Jaeger Junior
Universidade Federal do Rio Grande do Sul, Brasil

Prof. Dr. Evandro Barbosa
Universidade Federal de Pelotas, Brasil.

Profª. Drª. Gina Gouveia Pires de Castro
Universidade Federal de Pernambuco, Brasil

Prof. Dr. Gustavo Castagna Machado
Universidade Federal de Pelotas, Brasil

Prof. Dr. Jorge Núñez
Universidad de Buenos Aires, Argentina

Prof. Dr. José Alcebiades de Oliveira Junior
Universidade Federal do Rio Grande do Sul, Brasil

Profª. Drª. Laís Bergstein
Centro Universitário Curitiba, Brasil

Prof. Dr. Leomar Rippel
Universidade Federal de Rondônia, Brasil

Profª. Drª. Lucia Souza D'Aquino
Universidade Federal Fluminense, Brasil

Prof. Dr. Marco Antônio César Villatore
Universidade Federal de Santa Catarina, Brasil

Prof. Dr. Nitish Monebhurrin
Centro Universitário de Brasília, Brasil

Prof. Dr. Ricardo Sontag
Universidade Federal de Minas Gerais, Brasil

Profª. Drª. Tatiana de Almeida Freitas Rodrigues Cardoso Squeff
Universidade Federal do Rio Grande do Sul, Brasil

Profª. Drª. Thaís Cristina Alves da Costa
Universidade Comunitária da Região de Chapecó, Brasil

Prof. Dr. Wagner Silveira Feloniuk
Universidade Federal do Rio Grande, Brasil

Apresentação

O Centro de Ensino Superior CESUL se destaca no panorama educacional brasileiro ao oferecer uma sólida formação acadêmica e profissional, com especial atenção ao Bacharelado em Direito, curso mais longo da instituição. Para garantir a excelência em sua missão, o CESUL investe no desenvolvimento contínuo de seus docentes, incentivando tanto o aprimoramento didático quanto a produção de conhecimento, fortalecendo, assim, a cultura jurídica no Paraná e no Brasil.

A Direito em Revista desempenha um papel fundamental nesse contexto, selecionando criteriosamente artigos que buscam não apenas expandir as fronteiras da Ciência do Direito, mas também oferecer respostas reflexivas e inovadoras aos desafios jurídicos, políticos e sociais da atualidade. A publicação reúne produções de professores e alunos de programas de pós-graduação, estabelecendo-se como um espaço de diálogo acadêmico que promove a evolução do pensamento jurídico e contribui para o debate público qualificado.

Na 37ª edição, referente ao segundo semestre de 2024, a Direito em Revista reafirma seu compromisso com a excelência acadêmica ao publicar reflexões de relevância científica e social, fortalecendo o vínculo entre a pesquisa jurídica e as necessidades da sociedade brasileira.

Gustavo Ellwanger Calovi

IMPACTOS NA PRIVACIDADE, SEGURANÇA E CONFIANÇA NAS RELAÇÕES DIGITAIS NAS EMPRESAS: DESAFIOS E PERSPECTIVAS NA ERA DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI N. 13.709/2018)

IMPACTS ON PRIVACY, SECURITY AND TRUST IN DIGITAL RELATIONSHIPS IN COMPANIES: CHALLENGES AND PERSPECTIVES IN THE ERA OF THE GENERAL DATA PROTECTION LAW (LAW NO. 13.709/2018)

Luis Cesar Sell¹
Rangel Oliveira Trindade²

Resumo: O artigo científico analisou o impacto da Lei n. 13.709/2018, mais conhecida como Lei Geral de Proteção de Dados (LGPD), a legislação brasileira mais atual e relevante em relação à proteção de dados, que regula como os dados serão coletados e tratados. O presente estudo se baseia no método hipotético-dedutivo, com o procedimento embasado em pesquisa bibliográfica, envolvendo a análise de livros, artigos jurídicos, documentos legislativos e jurisprudência. A LGPD foi examinada como uma legislação que regulamenta o tratamento de dados pessoais por empresas e organizações no Brasil, com o objetivo de proteger a privacidade e os direitos dos indivíduos. O artigo explora como a implementação da LGPD afeta a confiança nas relações digitais

¹ Acadêmico de Direito, Associação Catarinense de Ensino - Faculdade Guilherme Guimbala.

² Doutor em Direito pela Universidade Federal do Paraná (UFPR), Mestre em Direito e Relações Internacionais pela Universidade Federal de Santa Catarina (UFSC), professor da Associação Catarinense de Ensino - Faculdade Guilherme Guimbala.

entre empresas e consumidores, ressaltando que a conformidade com a lei não é apenas uma obrigação legal, mas também uma oportunidade para as empresas fortalecerem a confiança de seus clientes. Além disso, discute-se as mudanças necessárias nas práticas empresariais, incluindo o reforço das medidas de segurança da informação, a criação de políticas de privacidade mais transparentes e o treinamento contínuo de funcionários sobre proteção de dados. Por fim, o artigo conclui com uma análise das perspectivas futuras da LGPD, incluindo possíveis ajustes na legislação, a evolução das práticas de proteção de dados e seu impacto em áreas como tecnologia, inovação e economia.

Palavras-chave: Lei Geral de Proteção de Dados; tratamento de dados; políticas de privacidade; empresas.

Abstract: The scientific article analyzed the impact of Law No. 13.709/2018, better known as the General Data Protection Law (LGPD), the most current and relevant Brazilian legislation concerning data protection, which regulates how data will be collected and processed. The present study is based on the hypothetical-deductive method, with the procedure grounded in bibliographic research, involving the analysis of books, legal articles, legislative documents, and case law. The LGPD was examined as legislation that regulates the processing of personal data by companies and organizations in Brazil, aiming to protect individuals' privacy and rights. The article explores how the implementation of the LGPD affects trust in digital relationships between companies and consumers, emphasizing that compliance with the law is not only a legal obligation but also an opportunity for companies to strengthen their customers' trust. Additionally, it discusses the necessary changes in business practices, including strengthening information security measures, creating more transparent privacy policies, and providing ongoing employee training on data protection. Finally, the article concludes with an analysis of the future perspectives of the LGPD, including potential adjustments to the legislation, the evolution of data protection practices, and its impact on areas such as technology, innovation, and the economy.

Keywords: General Data Protection Law; data processing; privacy policies; enterprises.

INTRODUÇÃO

Considera-se que o presente artigo tem como principal objetivo discorrer sobre os impactos na privacidade, segurança e confiança nas relações digitais empresariais, abordando os desafios e perspectivas na era da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018), bem como a importância da implantação nas empresas e seus impactos diretos da Lei Geral de Proteção de Dados.

A Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709/2018, representa um marco regulatório no Brasil no que diz respeito ao tratamento de dados pessoais. Ela foi criada com o objetivo de garantir a privacidade e a proteção dos dados dos cidadãos, estabelecendo normas claras sobre como as empresas e demais organizações devem coletar, armazenar, tratar e compartilhar essas informações.

Portanto, a definição do problema reside na compreensão dos desafios enfrentados pelas empresas na observância da LGPD e na análise dos impactos dessa conformidade ou falta dela na sociedade, abrangendo questões relacionadas à privacidade, segurança e confiança nas relações digitais. Entender como as empresas lidam com a LGPD e como isso repercute na sociedade é fundamental para promover um ambiente digital mais seguro, ético e transparente.

A perda de confiança dos clientes pode levar a uma diminuição das vendas, litígios, multas regulatórias e danos duradouros à imagem da marca. Portanto, é fundamental que as empresas estejam cientes das suas obrigações legais em relação à proteção de dados e tomem medidas proativas para garantir a conformidade e proteger a privacidade dos dados pessoais dos indivíduos. Parte superior do formulário

É importante destacar que, de acordo com a LGPD, tratamento de dados pessoais engloba uma ampla gama de atividades, incluindo a simples coleta, acesso, armazenamento, uso, compartilhamento e exclusão de dados pessoais; pois qualquer atividade que envolva dados que identifiquem direta ou indiretamente uma pessoa física está sujeita à lei.

Ressalte-se aqui que o objetivo específico deste estudo é analisar de que forma o cidadão brasileiro pode ter controle maior no tratamento de seus dados pessoais, e seus direitos fundamentais de liberdade de expressão, de informação, de comunicação, opinião, a inviolabilidade da intimidade, da honra e da imagem.

Além disso, pretende-se demonstrar e esclarecer infrações cometidas às normas previstas nesta Lei, que ficam sujeitos às sanções administrativas aplicáveis pela autoridade nacional. O objetivo geral é analisar, compreender e determinar quais medidas da Lei Geral n. 13.709/2018 foram implementadas nas empresas, sendo elas passíveis de condenação por danos materiais e morais.

O presente artigo está desenvolvido em 5 (cinco) capítulos, iniciando pela introdução e finalizando com as considerações finais e agradecimentos. O segundo capítulo abordará a temática sobre o Sistema Normativo de Proteção de Dados. O terceiro capítulo discutirá o Marco Civil da Internet. No quarto capítulo, será abordado o normativo da Lei Geral de Proteção de Dados, visando sua necessidade de proteção atualmente. No quinto capítulo, serão apresentados os procedimentos metodológicos. O sexto capítulo trará a análise de resultados.

Considerando que, na elaboração desta pesquisa, utilizar-se-á como forma de abordagem o método hipotético-dedutivo, comumen-

te associado à pesquisa científica, especialmente nas ciências naturais, reflete-se sobre a proteção dos dados pessoais sensíveis na Lei Geral de Proteção de Dados Pessoais. O método hipotético-dedutivo será aplicado com a utilização de técnicas de pesquisa bibliográfica e documental, mediante a utilização de livros, artigos científicos impressos e digitais, bem como da legislação específica sobre o tema.

A implementação da LGPD, no Brasil traz consigo uma série de mudanças estruturais tanto para as empresas quanto para a sociedade. Dada a sua complexidade e amplo alcance, podemos levantar algumas hipóteses sobre os impactos dessa legislação, tais como: maior proteção à privacidade dos cidadãos, melhoria na segurança dos dados pessoais, impacto na conformidades e nos custos operacionais, mudança na cultura dos tratamentos de dados, reforço à cidadania digital.

Com a exigência de consentimento explícito para a coleta e tratamento de dados pessoais, a sociedade passa a ter maior controle sobre suas informações. Essa mudança promove uma cultura de respeito à privacidade e aos direitos individuais, reforçando o papel do cidadão como dono de seus próprios dados e criando um ambiente de maior segurança em relação ao uso dessas informações por empresas e organizações.

Na era digital, proteger os dados pessoais tornou-se uma prioridade essencial para as empresas, especialmente com a chegada da Lei Geral de Proteção de Dados (LGPD). Essa lei busca assegurar que as organizações tratem as informações das pessoas de maneira ética e segura, respeitando o direito à privacidade.

Adaptar-se à LGPD não é simples. As empresas precisam rever seus processos internos, investir em tecnologia, capacitar seus colaboradores e reorganizar o fluxo de dados. Isso exige tempo, recursos e

uma mudança de mentalidade. A segurança da informação, por sua vez, é crítica nesse cenário: qualquer falha pode expor dados, comprometendo a reputação da empresa e acarretando multas pesadas.

Além disso, confiança é fundamental nas relações digitais. Clientes e parceiros estão cada vez mais atentos à forma como suas informações são utilizadas, e a transparência no tratamento dos dados virou uma exigência. Quem consegue mostrar compromisso com a privacidade acaba ganhando vantagem competitiva, fortalecendo sua reputação no mercado.

Olhando para o futuro, a necessidade de evoluir as regulamentações será constante, à medida que novas tecnologias surgem e trazem novos riscos. As empresas que forem proativas e investirem em conformidade e segurança estarão mais preparadas para enfrentar os desafios, evitando problemas legais e perdas de confiança.

1. SISTEMA NORMATIVO DA PROTEÇÃO DE DADOS

A proteção dos dados pessoais se tornou essencial na era digital, uma vez que informações sensíveis têm relação direta com a análise de perfil dos indivíduos e podem ser coletadas por meio de redes sociais, cartões de crédito, acessos a páginas da web, entre outros, fornecendo dados sobre gostos, preferências, padrões sociais, estilo de vida, idade e sexo, que podem ser utilizados para direcionar produtos e serviços ou até mesmo atividades ilícitas.

Essa vulnerabilidade surge do fato de que o aumento da eficiência muitas vezes depende do uso intensivo de dados pessoais, o que pode expor os consumidores a riscos de privacidade e segurança (Brasil,

2018). Assim, proteger esses direitos fundamentais em um ambiente digital se tornou uma prioridade, especialmente com a implementação de regulamentos como a Lei Geral de Proteção de Dados (LGPD).

Nesse sentido, a LGPD representa um avanço significativo para a proteção dos direitos dos indivíduos, especialmente em um mundo digital e interconectado. A era digital trouxe uma revolução nas relações empresariais, facilitando a comunicação, gestão de informações e promovendo a inovação. No entanto, com essas vantagens surgiram também desafios consideráveis, especialmente relacionados à privacidade, segurança e confiança nas interações digitais.

A Lei Geral de Proteção de Dados (Brasil, 2018), mais conhecida como LGPD, foi implementada no Brasil visando regulamentar o tratamento de dados pessoais, estabelecendo um marco legal rigoroso para garantir a privacidade dos indivíduos e a segurança das informações.

Para as empresas, a chegada da LGPD representou um marco significativo, exigindo uma reestruturação profunda de processos internos e sistemas tecnológicos. Adaptar-se às exigências da lei implica em investimentos em novas tecnologias, treinamento contínuo de colaboradores e revisão de políticas internas, tudo isso para garantir a conformidade legal.

Além disso, o cumprimento da LGPD transcende a mera legalidade, tornando-se uma questão crucial de confiança consumidores e parceiros esperam que as organizações tratem seus dados com a máxima responsabilidade e transparência, o que pode se traduzir em um diferencial competitivo no mercado. Nesse contexto, as empresas enfrentam o desafio de equilibrar a inovação tecnológica com a proteção

de dados, assegurando que suas práticas de segurança sejam robustas o suficiente para prevenir vazamentos e ataques cibernéticos.

Portanto, a confiança nas relações digitais emerge como um ativo estratégico, onde a transparência e a ética no manejo de informações pessoais são essenciais à construção e manutenção de uma boa reputação (Lima, C., 2019). Diante disso, os impactos da LGPD nas empresas são profundos e multifacetados.

Considerando que a era digital trouxe uma transformação significativa na forma como as empresas operam e interagem com seus clientes, parceiros e funcionários. Com o crescente uso de tecnologias da informação e comunicação, a coleta, armazenamento e processamento de dados pessoais tornaram-se práticas comuns e essenciais para a competitividade e inovação. No entanto, essa realidade também gerou preocupações crescentes sobre a privacidade, a segurança e a confiança nas relações digitais, especialmente no contexto corporativo.

Conforme Claudio Lóssio (2023, p. 220), “a publicação, em agosto de 2018, da LGPD mencionada, reforçou a necessidade das organizações em realizar investimentos em sua estrutura e em adotar políticas internas que atendam as exigências de segurança voltadas ao tratamento dos dados pessoais”. No entanto, questões persistem: as empresas estão realmente implantando corretamente a LGPD? Qual é a finalidade desses dados? Como vazamentos podem ser usados para chantagens e extorsões? E quem são os prejudicados diretos?

Conhecer esses aspectos permite avaliar com precisão como a legislação atual protege os direitos dos titulares de dados e como as empresas devem se adequar para evitar infrações e garantir a confiança dos consumidores (Brasil, 2018). Torna-se indispensável avaliar como o

cidadão brasileiro pode ter controle maior sobre o tratamento de seus dados pessoais, como a liberdade de expressão, informação, comunicação, opinião, de inviolabilidade da intimidade, honra e imagem. Desta forma, tende-se a demonstrar e esclarecer infrações cometidas às normas previstas nesta Lei, ficando sujeitos às sanções administrativas aplicáveis pela autoridade nacional (Brasil, 2021).

Conforme Doneda (2020), os avanços tecnológicos nas tecnologias de informação e mídia, o aumento do uso dos meios digitais e, conseqüentemente, dos computadores, aumentam a necessidade de proteção dos direitos fundamentais mais especificamente. À medida que os dados são usados para aumentar a eficiência econômica e a produção e distribuição de produtos, os proprietários de dados, geralmente consumidores de bens, tornam-se progressivamente vulneráveis (Brasil, 2018).

É de extrema importância ter cuidado com os dados que estão diretamente relacionados à análise do perfil dos indivíduos. Essas informações podem ser obtidas por meio de redes sociais, cartões de crédito, acessos a páginas da web, entre outros, revelando gostos e preferências, padrões sociais, estilo de vida, idade e sexo. Esses dados são utilizados para direcionar a oferta de produtos, serviços ou até mesmo para facilitar atividades ilícitas. Nesse contexto, conforme ensina Carlos Roberto Gonçalves:

O reconhecimento dos direitos da personalidade como categoria de direito subjetivo é relativamente recente, como reflexo da Declaração dos Direitos do Homem, de 1789 e de 1948, das Nações Unidas, bem como da Convenção Europeia de 1950. No âmbito do direito privado, sua evolução tem-se mostrado

lenta. No Brasil, têm sido tutelados em Leis especiais e principalmente na jurisprudência, a quem coube a tarefa de desenvolver a proteção à intimidade do ser humano, sua imagem, seu nome, seu corpo e sua dignidade (2011, p. 135).

Essa vulnerabilidade surge do fato de que o aumento da eficiência muitas vezes depende do uso intensivo de dados pessoais, o que pode expor os consumidores a riscos de privacidade e segurança (Brasil, 2018). Assim, proteger esses direitos fundamentais em um ambiente digital se tornou uma prioridade, especialmente com a implementação de regulamentos como a LGPD. Segundo Lima, Alcassa e Pappert:

O tratamento de dados pessoais ocorre quando há o recebimento e o acesso aos dados constantes: em currículos de candidatos; na coleta de informações e documentos adicionais para o processo de admissão de um empregado; na manutenção do contrato de trabalho; e até no compartilhamento de dados pessoais de empregados com alguns órgãos públicos, como a Receita Federal ou devido a alguns programas, como o e-social (2022, p. 18).

O sistema normativo de proteção de dados é constituído por um conjunto de leis, regulamentos e diretrizes voltados a assegurar a proteção e a privacidade das informações pessoais dos cidadãos. No cenário global, e especialmente no Brasil, com a implementação da Lei Geral de Proteção de Dados (LGPD), esse sistema tornou-se essencial para regular o tratamento de dados sensíveis pelas empresas e organizações.

Quando da vigência plena da LGPD, teremos um motivo adicional para buscar a proteção dos dados pessoais e sensí-

eis presentes em nossos sistemas, pois, além dos motivos e penalidades expostos na lei, antevemos um aumento das ocorrências de furtos de dados com o objetivo de extorsão (Pinheiro, 2020, p. 22).

A expressão “dado pessoal” traz em si boa parte do conceito jurídico. Dados, conforme o dicionário jurídico de Mara Helena Diniz (2003), são, no campo do direito de informática, os elementos fundamentais do sistema normativo, que inclui a LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) (Brasil, 2019), além de normas complementares e regulamentações setoriais, impactando significativamente na implementação e na aplicação das regras de proteção de dados.

Em síntese, o sistema normativo da proteção de dados, centrado na LGPD no Brasil, representa um avanço significativo na garantia de que as informações pessoais sejam tratadas de maneira ética e responsável, equilibrando o desenvolvimento tecnológico com a proteção dos direitos individuais e a promoção da confiança nas relações comerciais e sociais. Segundo Pinheiro (2020), segredos de negócios são objeto de ataque desde que o mundo é mundo. As revoluções industriais que se sucederam foram interferindo e mudando a dinâmica das relações humanas e comerciais, e o que presenciamos hoje não é diferente.

1.1 MARCO CIVIL DA INTERNET

O Marco Civil da Internet começou como um projeto de lei em 2011, com o número 2.126. Após um processo legislativo que envolveu a Câmara dos Deputados e o Senado Federal, a lei foi finalmente sancio-

nada pela presidência em 23 de abril de 2014 (Lucca; Simão Filho; Lima, 2015). Assim, a proposta foi transformada na Lei nº 12.965/14 (Brasil, 2014), que recebeu tanto críticas favoráveis quanto desfavoráveis.

As sanções administrativas da LGPD não se confundem com outros tipos de sanções previstas em outras leis, como Código de Defesa do Consumidor ou Marco Civil da Internet. Em outras palavras, as autoridades que aplicam estas últimas não têm competência para aplicar a primeira. A LGPD estabeleceu precisamente, em seu artigo 52, que as sanções serão aplicadas pela autoridade nacional, ou seja, a ANPD (Oliveira, 2021, p. 10).

O Marco Civil da Internet representou a primeira regulamentação específica das comunicações via internet no país e marcou um avanço significativo, pois o Brasil estava ficando atrás de outros países nessa área (Santarém, 2011). No entanto, a legislação não abordou a proteção da privacidade por meio da padronização da base de dados.

A LGPD estabeleceu os critérios para dosimetria da sanção: (i) a gravidade e a natureza das infrações e dos direitos pessoais afetados; (ii) a boa-fé do infrator; (iii) a vantagem auferida ou pretendida pelo infrator; (iv) a condição econômica do infrator; (v) a reincidência; (vi) o grau do dano; (vii) a cooperação do infrator; (viii) a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; (ix) a adoção de política de boas práticas e governança; (x) a pronta adoção de medidas corretivas; e, (xi) a proporcionalidade entre a gravidade da falta e a intensidade da sanção (Oliveira, 2021, p. 11).

Portanto, o Marco Civil da Internet não limitou direitos específicos ao uso e compartilhamento indevidos dos dados pessoais coletados nem ao seu uso para fins diversos daqueles originalmente pretendidos. A Lei nº 13.709, de 14 de agosto de 2018, mas conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), provocou um dos maiores reboiços jurídicos que se tem notícia nos últimos anos, (Oliveira, 2021, p. 7).

1.2 LEI GERAL DE PROTEÇÃO DE DADOS

O termo “proteção de dados” no Brasil só foi incorporado recentemente, mas sempre o associou à privacidade, aos direitos do consumidor e às liberdades individuais, a Lei Geral de Proteção de Dados é a legislação brasileira que determina a forma quanto os dados dos cidadãos podem ser tratados, e até agora prevê punições para transgressões a essas determinações (Mendes, 2020). No entanto, confiar apenas na “proteção da privacidade” não mais suporta a nova situação que surgiu após o surgimento das mídias virtuais, porque o direito à privacidade é um direito individual e subjetivo (Diniz, 2016).

A Lei nº 13.709/2018, conhecida como “Lei Geral de Proteção de Dados Pessoais” (LGPD), foi promulgada com o objetivo de proteger os dados pessoais, inspirando-se na GDPR (Regulamento Geral sobre a Proteção de Dados), que está em vigor na União Europeia desde 25 de maio de 2018, sendo aplicada a todos os países membros. A criação da LGPD visa preencher lacunas existentes e promover melhorias no tratamento de dados pessoais no ordenamento jurídico brasileiro.

A escolha do legislador seguiu o padrão europeu, que em seu regulamento (GDPR - Regulamento Geral sobre a Proteção de Dados - Regulamento (UE) 2016/679), tampouco dispõe acerca dessa questão e delega a um novo normativo apreciar o tema e definir os limites e possibilidade. Trata-se de uma escolha que demandará estudo e um balanceamento de direitos, conjuntamente com uma política pública própria, aplicada ao povo de cada país, considerando sua especificidade cultural (Soler, 2020, p. 11).

Portanto, visando evitar o processamento indevido desses dados por instituições públicas e privadas, foi iniciada a regulamentação desta matéria no Brasil. Rafael Fernandes Maciel, em sua obra “Manual Prático sobre a Lei Geral de Proteção de Dados”, conceitua a LGPD:

A LGPD dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, INCLUSIVE POR MEIO DIGITAL (2020, p. 17).

A implantação da Lei Geral de Proteção de Dados n. 13.709/2018 é de extrema importância para as empresas, considerando especialmente os impactos direto que ela pode ter. A LGPD estabelece regras claras para o tratamento de dados pessoais, garantindo que as empresas colem, armazenem, processem e compartilhem esses dados de forma segura e responsável. Isso é fundamental para proteger a privacidade e os direitos dos indivíduos, promovendo a confiança dos clientes e parceiros comerciais.

Isso porque, a proteção de dados é uma das formas para se proteger a privacidade da pessoa. Esse direito é parcela do Direito à Privacidade que está positivado em nossa Constituição Federal. É importante destacar que em 2020 o STF já se posicionou informando que o direito à proteção de dados é um direito fundamental e no final de 2021, a PEC 9 n. 17/2019 incluiu este direito expressamente no art. 5º, da Carta Magna, em razão da sua previsão difusa atualmente no texto constitucional (Soler, 2020, p. 9).

Conforme Ricardo Oliveira (2021, p. 19):

Vamos pensar, por exemplo, na gestão de currículos. Currículos não brotam do nada na empresa. Podem ser recebidos fisicamente, por meio de agentes terceiros, plataformas, e-mail, aplicativos, etc. No mapeamento por fluxo, o agente narra como recebe os currículos, onde, a partir daí, são armazenados, como funciona o momento da seleção, no qual o dado se multiplica em certa escala, pois é manuseado pelos profissionais envolvidos, como a rotina prossegue até o fechamento do contrato de trabalho, etc.

Acrescenta Pinheiro (2020, p. 125):

como não poderia deixar de ser, além do acesso a conteúdos corporativos da organização, durante a realização dos testes, pode ocorrer o acesso a informações referentes a pessoas físicas – colaboradores, clientes – e/ou a dados de fornecedores da organização.

Atualmente, o tratamento dos dados possui suma importância, pois oferece suporte aos mecanismos que evitam fraudes, sonegação e

práticas contrárias ao mercado, como a disponibilização de produtos e serviços com vantagens financeiras. Essas vantagens incluem preços e condições mais competitivos, acessíveis por meio do comércio eletrônico. Essa situação beneficia tanto o consumidor quanto a comunidade de maneira geral, para bem ou para mal. Segundo Pinheiro (2020, p. 115):

Concluiu-se que a proteção e defesa dos direitos e interesses individuais no contexto digital é atitude cabível no ordenamento jurídico brasileiro, mas deve ser observada com mais criteriosidade, zelo e cuidados, já que o ambiente digital apresenta mais desafios para a identificação exata do agressor, apresentando riscos que vão desde a perda da prova colhida para identificação do agente criminoso até mesmo às lesões a terceiros de forma colateral.

A fundamentação do direito trata da concretização jurídica de alguns dos direitos e garantias fundamentais da Constituição Federal de 1988 (Brasil, 1988). Como exemplo, cita-se o art. 2º, inciso I, que estabelece o respeito à privacidade como primeiro fundamento. Essa base particular atende integralmente ao inciso X do art. 5º da Constituição Federal, que adota as regras gerais de privacidade e inviolabilidade da privacidade, conforme o inciso IV do mesmo artigo na LGPD. Vale ressaltar que a introdução de práticas seguras no ambiente digital é uma das metas das autoridades brasileiras, conforme Oliveira (2021, p. 07):

Conforme o mercado já estava avisado de que um dia a LGPD geraria seus efeitos com plenitude, mas muitas empresas e órgãos públicos parecem que aguardaram o início das sanções administrativas para de fato se preocuparem com o tema. Para ser mais claro, a LGPD entrou em vigor no

dia 18 de setembro de 2020, ou seja, desde tal data todos os agentes de tratamento de dados pessoais já estavam sujeitos aos processos judiciais individuais ou coletivos que pudessem versar sobre os temas da nova lei.

De acordo com o art. 1º da LGPD (Brasil, 2018), a lei se aplica a todo e qualquer tratamento de dados, por qualquer meio, seja realizado por pessoa natural ou pessoa jurídica de direito público ou privado:

Art. 1º. A lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

É necessário que as organizações estejam em conformidade com as disposições da LGPD, o que geralmente envolve a implementação de políticas e procedimentos específicos para garantir a proteção adequada dos dados pessoais e o cumprimento das obrigações legais estabelecidas pela lei (Castells, 2006; Lóssio, 2023). O descumprimento das disposições da LGPD pode resultar em sanções e multas significativas.

O Artigo 2º da LGPD (Brasil, 2018) afirma claramente que a tarefa da lei é explicar aos responsáveis pelo tratamento de dados quais são as qualificações necessárias, preparar o caminho para alcançá-las e ser responsável por como devem ser cumpridas (Bruno, 2020). Dessa forma, é proporcionado às empresas um tempo maior para se adequarem à lei sem temer as penalidades mais severas da LGPD. No entanto,

o objetivo da referida lei é combinar os interesses de pessoas jurídicas, processadores de dados, e pessoas físicas, titulares de dados.

Artigo 2º - inciso 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 (xviii) (Brasil, 2018).

Estas razões, entre outras, referem-se à concretização legal de certos direitos e garantias previstos na Constituição (Brasil, 1988), o que levou o legislador a enumerar uma lista cumulativa de razões para proteger os dados pessoais. Segundo Ricardo Olivera (2021, p. 8):

A lista de medidas corretivas, a meu ver, é exaustiva, ou seja, a ANPD (Autoridade Nacional de Proteção de Dados) não poderia aplicar sanções diferentes ou não previstas na LGPD, ainda que entenda que sua aplicação favoreceria o cumprimento da lei no futuro, como é o caso de aplicar uma multa bilionária sobre as empresas com alta capacidade financeira, só por considerar que o teto de 50 milhões de reais ser considerado baixo para elas. Nesse caso a autoridade dispõe de outros tipos de sanção e sua escolha deve se fazer com inteligência.

Embora não sejam inovações legislativas, é importante que existam para orientar a aplicação da LGPD, impondo requisitos específicos de conformidade que devem ser seguidos, incluindo a necessidade

de obter consentimento explícito para o processamento de dados pessoais, a designação de um encarregado de proteção de dados (DPO), a implementação de medidas de segurança adequadas e a notificação de violações de dados. A não conformidade com a LGPD pode resultar em penalidades significativas, incluindo multas financeiras que podem chegar a até 2% (dois por cento) do faturamento anual da empresa, limitado a R\$ 50 milhões por infração (Brasil, 2018).

1.3 RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS

O delito sempre foi objeto de investigação, mas a forma de infração por quebra de dever mudou ao longo da história do Direito Civil. Além disso, a origem do sistema de responsabilidade está fundamentada no conceito de vingança privada (Gagliano; Pamplona Filho, 2006). A responsabilidade civil é um regime pertencente ao ramo do Direito Obrigacional, que decorre do reconhecimento dos direitos das pessoas. Este regime regula a relação entre as pessoas para prevenir a violação dos direitos humanos.

Nas sociedades primitivas, a resposta ao comportamento lesivo caracteriza-se pela autopreservação, ou seja, a vítima ou seu grupo, sem quaisquer restrições estatais, vinga-se do agressor. Com princípio de um por um, a punição é proporcional ao dano causado. Posteriormente, a principal forma de reparação dos danos passou a ser a indenização pecuniária (Farias; Braga Netto; Rosenvald, 2015, p. 27).

Danos no âmbito civil são atos ilícitos que geram obrigação de ressarcimento. Assim, cria-se uma limitação legal que confere a uma das partes o direito de exigir da outra parte o cumprimento de determinadas condições (Gonçalves, 2011). É importante detalhar os elementos e tipos de responsabilidade existentes, pois isso é fundamental para discutir a responsabilidade civil no contexto da proteção de dados pessoais. Atualmente, com base no positivismo jurídico, os conceitos de responsabilidade estão evoluindo conforme as consequências dos eventos danosos.

A responsabilidade penal envolve a punição pessoal do agente responsável, enquanto a responsabilidade civil trata da reparação do dano (Gagliano; Pamplona Filho, 2006). A legislação brasileira atual, no que se refere à responsabilidade civil, prevê a reparação de danos por atos ilícitos conforme o art. 927 do Código Civil Brasileiro: “Aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo” (Brasil, 2002). Gagliano e Pamplona Filho (2006, p. 54) conceituam a responsabilidade civil da seguinte maneira:

Trazendo esse conceito para o âmbito do Direito Privado, e seguindo essa mesma linha de raciocínio, diríamos que a responsabilidade civil deriva da agressão a um interesse eminentemente particular, sujeitando, assim, o infrator, ao pagamento de uma compensação pecuniária à vítima, caso não possa repor *in natura* o estado anterior de coisas.

A mesma lógica segue o Direito Civil ao definir o objeto em termos de responsabilidade civil contratual. O artigo 389 do Código Civil estabelece que “em caso de descumprimento das obrigações, o devedor

responderá por perdas e danos, juros e correção monetária, segundo índice oficial regularmente estabelecido, e custas judiciais” (Brasil, 2002).

Por conseguinte, a responsabilidade civil decorre do não cumprimento de determinado dever (Brasil, 2002), Cavalieri Filho (2015) explica que a responsabilidade civil é uma obrigação legal contínua, que surge do descumprimento de uma obrigação preexistente (isto é, a obrigação legal originária). Assim, a responsabilidade civil inclui a obrigação de reparar os danos causados pelo descumprimento dessa obrigação.

Neste contexto, a questão do dano exige que este seja devidamente comprovado pelo titular dos dados pessoais. Portanto, é necessário considerar no caso concreto se as partes envolvidas estão sujeitas a uma violação material de seus direitos como resultado da conduta do subcontratante e se essa conduta constitui uma violação material da norma legal.

1.4 IMPACTOS NA PRIVACIDADE, SEGURANÇA E CONFIANÇA NAS RELAÇÕES DIGITAIS NAS EMPRESAS

Com a crescente digitalização dos negócios, as empresas estão mais dependentes do que nunca das tecnologias digitais para suas operações diárias. Isso trouxe inúmeros benefícios, como maior eficiência e alcance de mercado. No entanto, também surgiram preocupações significativas em relação à privacidade, segurança e confiança nas relações digitais.

Todas essas práticas são realizadas para que o risco da empresa seja o mínimo possível. Todavia, esse risco nunca será

igual a zero já que, como aponta Tácito Leite, “não existe sistema ou software, por mais avançado que seja, que resolva por si questões relacionadas a riscos e defina sozinho qual a melhor decisão a ser tomada”. Isso significa que existem algumas partes do processo de segurança que – ao menos ainda – devem ser avaliadas pela subjetividade humana; por conta disso, além de um aparato de segurança eficaz, é preciso ter uma equipe de gestão de segurança muito bem preparada e pronta para lidar com as reais necessidades da empresa (Pinheiro, 2020, p. 42).

A privacidade dos dados se tornou uma preocupação central à medida que as empresas coletam, armazenam e processam grandes volumes de informações pessoais e sensíveis. Os principais impactos na privacidade incluem: a) Coleta excessiva de dados: muitas empresas acabam coletando mais dados do que o necessário, aumentando os riscos em caso de vazamentos ou uso indevido; b) Uso indevido de dados: informações pessoais podem ser usadas para fins que não foram autorizados pelos indivíduos, como marketing agressivo ou vendas de dados; c) Vazamentos de dados: incidentes de segurança que expõem informações pessoais podem causar danos significativos aos indivíduos afetados e à reputação da empresa.

As relações digitais nas empresas apresentam desafios significativos para a privacidade, segurança e confiança. No entanto, com práticas adequadas de gerenciamento e uma abordagem proativa, é possível minimizar os riscos e construir uma base sólida de confiança com clientes e parceiros. A segurança cibernética e a privacidade devem ser prioridades estratégicas para qualquer empresa que busca prosperar na era digital.

Além disso, os impactos da observância da LGPD não se limitam apenas ao âmbito empresarial, mas se estendem à sociedade como um todo. A conformidade com a LGPD influencia diretamente a maneira como as empresas lidam com os dados dos indivíduos, afetando sua privacidade, liberdade e segurança digital (Paesani, 2014). Por outro lado, a não conformidade pode resultar em violações de dados, vazamentos de informações sensíveis e violações de direitos fundamentais dos cidadãos (Santarém, 2011).

1.5 PRINCÍPIOS APLICADOS AO TRATAMENTO DE DADOS PESSOAIS

Considerando de que os princípios aplicados ao tratamento de dados pessoais são fundamentais para garantir que as informações dos indivíduos sejam coletadas, armazenadas e utilizadas de forma ética e segura. Esses princípios estabelecem diretrizes que as empresas e organizações devem seguir para garantir o respeito à privacidade e à proteção dos dados, especialmente em conformidade com a Lei Geral de Proteção de Dados. Conforme destaca Pinheiro:

A regulamentação de proteção de dados pessoais é uma legislação principiológica, como já foi dito. Sendo assim, tanto na origem europeia como na versão nacional traz um rol de princípios que precisam ser atendidos. A melhor forma de analisar a lei é pela verificação da conformidade dos itens de controle, ou seja, se o controle não está presente, aplicado e implementado, logo o princípio não está atendido (Pinheiro, 2023, p. 37).

O Regulamento Geral de Proteção de Dados (RGPD), que entrou em vigor em 25 de maio de 2018, estabelece diretrizes rigorosas para o tratamento de dados pessoais, com o objetivo de proteger a privacidade dos indivíduos (Pestana, 2020). O artigo 5º do GDPR elenca os princípios fundamentais que orientam esse tratamento. Entre os princípios, destacam-se a legalidade, transparência, minimização dos dados, exatidão, limitação da finalidade e segurança.

Pela LGPD, as atividades de tratamento legítimo, específico e explícito de dados pessoais informado previamente ao titular devem estar orientadas pelos seguintes princípios: finalidade, adequação, necessidade, livre acesso, transparência, segurança, responsabilização e prestação de contas (Pinheiro, 2023).

1.5 MEDIDAS PRÁTICAS PARA SE EVITAR SANÇÕES

Considerando evitar avaliações relacionadas ao tratamento de dados pessoais, é essencial adotar uma série de medidas práticas e homologadas às regulamentações de privacidade, como o Regulamento Geral sobre a Proteção de Dados. A LGPD criou a figura do Encarregado de tratamento de dados pessoais, conhecida no exterior como Data Protection Officer (DPO). Segundo a definição legal do artigo 5º, inciso VIII, o encarregado é a “pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)” (Oliveira, 2021).

A principal função do encarregado é citada em sua definição, que é justamente servir de ponto de referência para que se

saiba a quem as demandas relacionadas ao tratamento de dados pessoais devem ser direcionadas. A intenção do legislador é clara: quando o assunto é tratamento de dados, não deve haver dúvidas sobre quem acionar – a pessoa responsável por receber os pedidos internos é o encarregado (Oliveira, 2021, p.16).

2. PROCEDIMENTOS METODOLÓGICOS

Na elaboração desta pesquisa, será adotado, como forma de abordagem, o método hipotético-dedutivo, comumente associado à pesquisa científica, especialmente nas ciências naturais, para refletir sobre a proteção dos dados pessoais sensíveis na Lei Geral de Proteção de Dados Pessoais. O objetivo será estabelecer a tutela efetiva dos dados pessoais sensíveis à saúde, visando proteger uma dimensão dos direitos da personalidade (Diniz, 2016). O método hipotético-dedutivo será empregado em conjunto com a utilização de técnicas de pesquisa bibliográfica e documental, utilizando livros e artigos científicos impressos e digitais, bem como da legislação específica pertinente ao tema (Lüdke; André, 1986).

Esse método envolve a formulação de hipóteses fundamentadas em observações ou teorias já existentes e, posteriormente, a realização de testes para verificar essas hipóteses por meio de experimentação ou observação controlada (Denzin; Lincoln, 2006). O processo se inicia com a identificação de um problema ou uma lacuna no conhecimento científico, ou seja, quando o conhecimento disponível sobre um determinado tema é insuficiente para explicar um fenômeno, originando assim uma questão a ser investigada (Silva, 2014).

Dessa forma, para que se cumpram as regulamentações, as organizações geralmente precisam implementar medidas para proteger os dados pessoais, nomear um Encarregado de Proteção de Dados (DPO), realizar avaliações de impacto na privacidade, obter consentimento para o processamento de dados, garantir os direitos do titular dos dados e implementar medidas de segurança para proteger os dados pessoais.

Considerando que o presente artigo busca aprimorar o desenvolvimento e a compreensão da pesquisa, utiliza-se o método de pesquisa bibliográfica, que envolve a análise de livros, artigos jurídicos, documentos legislativos e jurisprudência. Esse enfoque é fundamental para entender a natureza jurídica e os limites da responsabilidade civil no contexto da proteção de dados pessoais (Gil, 2008). Ademais, comparar as regras gerais da responsabilidade civil com as específicas aplicáveis à proteção de dados é essencial para compreender o tema e para elaborar soluções práticas e juridicamente fundamentadas.

3. ANÁLISE DE RESULTADOS

Visto que a LGPD é uma legislação recente, ainda há muita incerteza sobre a forma mais apropriada para sua aplicação. A LGPD inaugura uma nova cultura de privacidade e proteção de dados no país, exigindo a conscientização de toda a sociedade sobre a importância e o cuidado extremo que se deve ter com os dados pessoais e seus reflexos em direitos fundamentais como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural (Paesani, 2014; Diniz, 2016).

Independentemente do tamanho da empresa ou de sua natureza, a responsabilidade sobre a gestão (ou utilização) de dados e informações de colaboradores, clientes, fornecedores e órgãos públicos estava sob análise das autoridades governamentais, especialmente as brasileiras, há muito tempo (Lima, C., 2015).

Portanto, a definição do problema reside na compreensão dos desafios enfrentados pelas empresas na observância da LGPD e na análise dos impactos dessa conformidade ou falta dela na sociedade, abrangendo questões relacionadas à privacidade, segurança e confiança nas relações digitais (Lóssio, 2023). Entender como as empresas lidam com a LGPD e como isso repercute na sociedade é fundamental para promover um ambiente digital mais seguro, ético e transparente.

A perda de confiança dos clientes pode levar a uma diminuição das vendas, litígios, multas regulatórias e danos duradouros à imagem da marca. Portanto, é fundamental que as empresas estejam cientes das suas obrigações legais em relação à proteção de dados e tomem medidas proativas para garantir a conformidade e proteger a privacidade dos dados pessoais dos indivíduos (Lóssio, 2023).

É importante destacar que, conforme a LGPD, tratamento de dados pessoais engloba uma ampla gama de atividades, incluindo a simples coleta, acesso, armazenamento, uso, compartilhamento e exclusão de dados pessoais. Sendo assim, qualquer atividade que envolva dados que identifiquem, direta ou indiretamente, uma pessoa física, está sujeita à lei (Bruno, 2020).

Cada vez mais, as empresas tendem a adotar medidas técnicas e administrativas para garantir a segurança dos dados, eliminar dados quando não forem mais necessários e cumprir os direitos dos titulares

dos dados. Esses aspectos são essenciais para a conformidade com as leis de proteção de dados (Oliveira, 2021). Além disso, fornecer informações claras e precisas sobre como os dados são tratados pela empresa é fundamental para construir confiança com os clientes e demonstrar transparência.

A adequação à LGPD é extremamente importante para garantir a devida proteção dos dados pessoais dos titulares e evitar sanções administrativas e financeiras que a ANPD possa impor. Manter a privacidade dos dados pessoais vem se tornando cada vez mais um grande desafio para os gestores de Departamentos de Segurança da Informação de empresas de diversos tamanhos e nichos de negócio (Oliveira, 2021).

Os danos à reputação de uma empresa devido a violações de dados ou falta de conformidade com as leis de proteção de dados podem ser significativos e difíceis de reparar. Atualmente, é prática comum em praticamente todas as empresas comerciais de atacado e varejo, incluindo bares, restaurantes e similares, solicitar o CPF e número de telefone do cliente para cadastro posterior.

Adicionalmente, registros processuais, que deveriam ser sigilosos, estão disponíveis para qualquer pessoa, sem critérios e responsabilidade, deixando os cidadãos vulneráveis e com seus dados expostos, o que representa um grave problema em todas as esferas dos tribunais. Em qualquer momento, qualquer pessoa pode ter acesso a esses dados, sem critérios e responsabilidade, tornando os cidadãos totalmente vulneráveis, com informações que deveriam estar protegidas e armazenadas de forma segura.

A observância da Lei Geral de Proteção de Dados, Lei n. 13.709 (Brasil, 2018), pelas empresas e seus impactos na sociedade apresenta-

-se como um desafio significativo no contexto contemporâneo. A LGPD estabelece diretrizes claras para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais, visando proteger a privacidade e a segurança das informações dos cidadãos.

Os avanços tecnológicos da era digital fizeram com que os dados recolhidos pelas empresas e organizações (públicas e privadas) se tornassem padrões dinâmicos para o setor financeiro. Essa transformação exigiu uma nova visão, na qual a informação é um bem valioso que deve ser protegido com prioridade máxima. Com o advento da era digital, diversos países reconheceram a necessidade de regulamentar a disponibilidade, o acesso e a utilização de recursos, dados e questões pessoais por meio de recursos legais.

A orientação emitida pela LGPD foi publicada para que as instituições e organizações enfrentassem a obrigação de cumprir honestamente as leis de tratamento de dados. O objetivo é criar os direitos fundamentais de privacidade, ética e proteção da liberdade, com base no princípio da transparência. No entanto, a implementação efetiva da LGPD por parte das empresas pode encontrar obstáculos diversos, que vão desde questões técnicas e operacionais até desafios culturais e organizacionais.

A falta de conhecimento sobre as exigências da lei, recursos limitados para adaptação dos processos internos e resistência à mudança são apenas alguns dos desafios enfrentados pelas organizações. Buscar o cumprimento das leis gerais de proteção de dados pessoais tornou-se uma grande preocupação para as organizações, principalmente as autoridades públicas que armazenam grandes quantidades de dados pessoais e estão envolvidas em atividades de processamento de dados.

Vários fatores, como humanos, técnicos ou regulatórios, entre outros, estão diretamente ligados ao êxito na implementação da LGPD. Para garantir a proteção dos dados pessoais de toda conduta ilícita — que vai desde acesso não autorizados, destruição, perda, alteração, comunicação —, tem-se que incentivar a prática de medida administrativas e cumprir todos os procedimentos que a legislação atual sobre a LGPD determina. Para que isso ocorra, tem-se que seguir à risca o princípio da transparência (Oliveira, 2021).

Sendo que somente as empresas em conformidade com a LGPD não estarão sujeitas às penalidades a serem aplicadas em caso do descumprimento das obrigações para com a privacidade dos dados classificados como alcançáveis pela lei, que vão desde a advertência, multas até a proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados, estas previstas na LGPD e que podem inviabilizar a continuidade da operação da empresa.

Para garantir a proteção dos dados pessoais contra condutas ilícitas, como acesso não autorizado, destruição, perda, alteração e comunicação indevida, é crucial que as empresas adotem medidas administrativas adequadas e cumpram rigorosamente os procedimentos estabelecidos pela legislação atual sobre a LGPD (Brasil, 2018).

A conformidade estrita com a LGPD é fundamental para evitar as penalidades aplicáveis em caso de descumprimento das obrigações de privacidade dos dados estabelecidas pela lei, que incluem advertências, multas e até mesmo a proibição parcial ou total das atividades relacionadas ao tratamento de dados.

Essas penalidades podem representar um risco significativo para a continuidade das operações da empresa. Para que ocorra a con-

tinuidade do negócio da empresa em função da responsabilidade para com os dados que mantém e/ou administra, a correta orientação à empresa quanto à tratativa dos dados por ela utilizados torna-se crucial à sua sobrevivência no mercado em que atua.

Visto que por estar na era da economia de dados, os dados dos clientes é grande ativo das empresas. Esses ativos então têm que ter proteção diferenciada, pois os dados são emprestados e informados às empresas, mas não são de propriedade delas e sim do cliente. Isso deve ser deixado claro.

Por isso tais dados têm que ser protegidos, preservados pois somente assim as empresas tendem a ter maior credibilidade, demonstrando assim maior transparência com dados que coletam, mostrando a real finalidade, quem é o seu processador e assim por diante. Sendo que os princípios da LGPD procuram enfatizar o respeito à privacidade, à liberdade de expressão, à integridade da intimidade, à livre iniciativa, à defesa do consumidor, aos direitos humanos, à dignidade e ao exercício dos direitos civis (Brasil, 2018).

Considerando de que a LGPD surgiu para ser aplicada a governos e empresas, com a principal finalidade de aumentar a segurança dos dados pessoais, respeitando os princípios fundamentais estabelecidos em lei e as diversas regras que hoje são padrão (fazer, finalidade, relevância, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilidade e toda responsabilidade relacionada aos dados pessoais). Reconhece-se a existência de proteção legislativa dos dados pessoais sensíveis, mas aponta-se para a necessidade de haver proteção efetiva desses dados, especialmente no que tange a saúde

por parte dos agentes de tratamento, empresas, instituições e governos (Coronavírus, 2020).

CONSIDERAÇÕES FINAIS

A implementação da Lei Geral de Proteção de Dados (LGPD) no Brasil trouxe consigo um novo paradigma nas relações digitais entre empresas, consumidores e o mercado como um todo. Ao estabelecer um conjunto de normas rigorosas para a coleta, tratamento e armazenamento de dados pessoais, a LGPD não só visa garantir a privacidade dos cidadãos, mas também reforçar a segurança e a confiança nas interações que permeiam o ambiente digital.

Considerando de que a lei geral de proteção de dados pessoais decorre da necessidade de assegurar os direitos básicos das pessoas, especialmente a privacidade e a intimidade da vida privada, pois disposições especiais para regular a responsabilidade por danos relacionados ao processamento de dados pessoais, cujas definições são provavelmente as mais amplas. O leque de atividades relacionadas com o tratamento de dados pessoais é muito diversificado e heterogêneo, pois, para alguns subcontratantes, o papel dos dados pessoais é fulcral para o cumprimento das obrigações.

As empresas enfrentam desafios significativos à medida que precisam adequar seus processos internos para atender às exigências da legislação. Entre os principais desafios está a necessidade de investir em sistemas de segurança cibernética robustos, capazes de proteger informações sensíveis contra vazamentos, ataques hackers e outras formas

de violação de dados. Além disso, é imperativo promover uma cultura organizacional que valorize a privacidade, envolvendo treinamento de funcionários e a reavaliação de políticas de governança corporativa.

Outro impacto relevante está na construção de confiança entre consumidores e empresas. Em um ambiente onde o tratamento dos dados se torna cada vez mais central nas operações empresariais, as organizações que demonstrarem transparência e comprometimento com a proteção das informações pessoais terão uma vantagem competitiva, consolidando-se como marcas confiáveis e responsáveis.

Por outro lado, a conformidade com a LGPD traz uma série de desafios técnicos e financeiros, que, especialmente para as pequenas e médias empresas, podem se tornar obstáculos significativos na implementação das mudanças necessárias. Isso se deve, em grande parte, a limitações orçamentárias e à falta de expertise técnica. Nesses casos, a assistência de consultorias especializadas e a colaboração com parceiros estratégicos podem ser essenciais para garantir a conformidade com as normas legais, sem comprometer o crescimento e a inovação.

Em termos de perspectivas futuras, a adoção plena da LGPD tem o potencial de fortalecer o ecossistema digital brasileiro, promovendo um ambiente mais seguro e ético para a utilização de dados pessoais. Com a crescente conscientização dos consumidores sobre seus direitos, espera-se uma pressão cada vez maior sobre as empresas para que mantenham um comportamento proativo em relação à privacidade e segurança.

Em resumo, a era da LGPD apresenta um cenário desafiador, mas também repleto de oportunidades. Empresas que souberem equilibrar inovação com conformidade e que adotarem uma postura ética e transparente no tratamento dos dados estarão mais preparadas para se

destacar em um mercado onde a confiança digital será um dos principais pilares para o sucesso.

A LGPD é um mecanismo de apoio fundamental para prevenção de danos e privacidade, mesmo em ambientes virtuais ilimitados. A complexidade desses padrões é desafiadora, mas é essencial que os segurados os entendam para defender seus direitos em juízo e com seus representantes, e para prevenir e reduzir o risco de possíveis ações legais.

Embora a Lei Geral de Proteção de Dados seja deliberadamente econômica em seu modelo adotado de responsabilidade e proteção de indivíduos e grupos, a natureza jurídica da responsabilidade é, na visão apresentada, subjetiva. Sua estrutura legal promove um sistema logicamente integrado projetado para proteger a mesma qualidade, descentralizada e individual com interesses coletivos.

A implementação da LGPD trouxe desafios significativos para as empresas brasileiras, mas também abriu novas oportunidades para melhorar a gestão de dados, a segurança da informação e a confiança nas relações digitais. As organizações que conseguiram se adaptar e integrar a conformidade com a LGPD em suas operações diárias não apenas atenderam às exigências legais, mas também fortaleceram sua posição no mercado. A era da LGPD está apenas começando, e as empresas que continuarem a investir em privacidade, segurança e transparência, estarão bem posicionadas para prosperar no ambiente digital em constante evolução.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definições dos agentes de tratamento de dados pessoais e do encarregado**. Brasília, DF: ANPD, 2021.

23 p. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 20 maio 2024.

_____. **Constituição da República Federativa do Brasil de 1988**.

Brasília, DF: Presidência da República, [1988]. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 29 jul. 2024.

_____. **Lei 10.406, de 10 de janeiro de 2002**. Institui o Código Civil.

Brasília, DF: Diário Oficial da União, [2002]. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/10406compilada.htm. Acesso em: 29 jun. 2024.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. In: VADE Mecum Compacto de Direito Rideel. São Paulo: Rideel, 2016.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Redação dada pela Lei nº 13.853, de 2019. Brasília, DF: Congresso Nacional, [2018]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 02 jul. 2024.

_____. **Lei nº 13.853, de 14 de agosto 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. Brasília, DF: Congresso Nacional, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 26 jun. 2024.

BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **Lei geral de proteção de dados comentada**. 2. ed. rev. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2020.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. *In: _____*; CARDOSO, Gustavo (org.). **A sociedade em rede**: do conhecimento à ação política. Lisboa, PRT: Imprensa Nacional: Casa da Moeda, 2006. p. 17-61.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil**. 12. ed. rev. e ampl. São Paulo: Atlas, 2015.

CORONAVÍRUS: Brasil confirma primeiro caso da doença. **UNA-SUS**, 2020. Disponível em: <https://www.unasus.gov.br/noticia/coronavirus-brasil-confirma-primeiro-caso-da-doenca>. Acesso em: 03 jun. 2024.

DENZIN, Norman Kent; LINCOLN, Yvonna Sessions. Introdução: a disciplina e a prática da pesquisa qualitativa. *In: _____* (org.). **O planejamento da pesquisa qualitativa**: teorias e abordagens. 2. ed. Porto Alegre: Artmed, 2006. p. 15-41.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: Responsabilidade civil. 17. ed. São Paulo: Saraiva, 2003.

_____. Direitos da Personalidade. *In: Curso de Direito Civil Brasileiro*: Teoria geral do Direito Civil. 33. ed. São Paulo: Saraiva, 2016. p. 131-161.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da lei geral de proteção de dados. 2. ed., rev. e atual. São Paulo: Revista dos Tribunais, 2020.

FARIAS, Cristiano Chaves de; BRAGA NETTO, Felipe Peixoto; ROSENVALD, Nelson; **Novo Tratado de Responsabilidade Civil**. 4. ed. Rio de Janeiro: Grupo GEN: Saraiva Jur, 2019. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788553612086/>. Acesso em: 07 out. 2024.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo curso de direito civil**: responsabilidade civil. 4. ed. rev. e atual. São Paulo: Saraiva, 2006. v. 3.

GIL, Carlos Antonio. **Métodos e Técnicas de Pesquisa Social**. 6. ed. São Paulo: Atlas, 2008.

GONÇALVES, Carlos Roberto. **Direito civil brasileiro**: responsabilidade civil. 7. ed. São Paulo: Saraiva, 2011. v. 7.

LIMA, Adrienne; ALCASSA, Flávia; PAPPERT, Milena (coord.). **LGPD no Direito do Trabalho**. São Paulo: Expressa, 2022. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786553621954/>. Acesso em: 10 out. 2024.

LIMA, Cíntia Rosa Pereira de. **A imprescindibilidade de um órgão independente para a efetiva proteção dos dados pessoais no cenário futuro do Brasil**. 2015. Tese (Livre Docência). Faculdade de Direito, Universidade de São Paulo (FRDP/USP), Ribeirão Preto, 2015. 487 p.

_____. (coord.). **Comentários à Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018)**. São Paulo: Almedina, 2019.

LÓSSIO, Claudio Joel Brito. **Proteção de dados e conformidade digital**. 2. ed. São Paulo: Grupo Almedina, 2023. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786556279893/>. Acesso em: 10 out. 2024.

LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). **Direito & internet**: marco civil da internet (Lei nº 12.965/2014). São Paulo: Quartier Latin, 2015. 2 v.

LÜDKE, Menga; ANDRÉ, Marli Eliza Dalmazo Afonso de. **Pesquisa em educação**: abordagens qualitativas. São Paulo: EPU, 1986.

MACIEL, Rafael Fernandes. **Manual prático sobre a Lei Geral de Proteção de Dados (Lei nº 13.709/18)**. Goiânia: RM Digital Education, 2020.

MENDES, Soraia da Rosa; MARTÍNEZ, Ana Maria. **Pacote Anticrime**: comentários críticos à Lei 13.964/2019. São Paulo: Grupo GEN: Atlas, 2020. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9788597025002/>. Acesso em: 07 out. 2024.

OLIVEIRA, Ricardo. **LGPD**: Como evitar as avaliações administrativas. Rio de Janeiro: Expressa, 2021. *E-book*. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786553621954/>.

da.minhabiblioteca.com.br/reader/books/9786553623262/. Acesso em: 07 out. 2024.

PAESANI, Liliana Minardi. **Direito e internet**: liberdade de informação, privacidade e responsabilidade civil. 7. ed. São Paulo: Atlas, 2014.

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

_____. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 4. ed. atual. e ampl. Rio de Janeiro: Saraiva Jur: Grupo GEN, 2023. Disponível em: <https://integrada.minhabiblioteca.com.br/reader/books/9786555599480/>. Acesso em: 10 out. 2024.

PESTANA, Nuno. **RGPD**: Regulamento Geral de Proteção de Dados. São Paulo: Vida Económica, 2020.

SANTARÉM, Paulo Rená da Silva. **O direito achado na rede**: a emergência do acesso à Internet como direito fundamental no Brasil. 2011. 158 f. Dissertação (Pós-Graduação em Direito). Faculdade de Direito, Universidade de Brasília (UnB), Brasília, 2010. Disponível em: <http://repositorio2.unb.br/jspui/handle/10482/8828>. Acesso em: 02 jul. 2024.

SILVA, Guilherme Leonardo Freitas; KNECHTEL, Maria do Rosário. Metodologia dapesquisa em educação: uma abordagem teórico-prácticadialogada. Curitiba: Intersaberes, 2014. **Práxis Educativa**, [S. l.], v. 11, n. 2, p. 531-534, 2017. DOI: 10.5212/PraxEduc.v.11i2.0013. Acesso em: 02 maio. 2024.

SOLER, Fernanda Galera. Pandemia e o início da vigência da Lei Geral de Proteção de Dados. **Revista dos Tribunais**, v. 109, n. 1022, p. 161-173, dez. 2020.

